

**FRAMEWORK TO MITIGATE SECURITY
VULNERABILITY (DENIAL OF SERVICE (DOS))
OF SESSION INITIATION PROTOCOL / VOICE
OVER INTERNET PROTOCOL (SIP /VOIP)**



By

Saqib Khalid

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

September 2017

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Saqib Khalid

DEDICATION

"In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my family and teachers, who supported me each step of the
way.

ABSTRACT

VoIP (Voice over Internet Protocol) is a technology that allows standard telephone voice signals to be compressed into data packets for transmission over the Internet or other IP network. VoIP is a combination of various protocols, integrated together to provide voice communication over internet or intranet environment. It offers higher flexibility and more features than traditional telephony (Public Switched Telephone Network (PSTN)) infrastructures, as well as the potential for lower cost and flexibility for consumer market. Because of these advantages, VoIP technology is rapidly evolving and is being integrated into many corporate and enterprises as a substitute or as a redundancy providing medium with PSTN. Session Initiation Protocol (SIP) is the corner stone of VoIP architecture; on the basis of it entire structure is VoIP communication infrastructure is created. Because of complexities of integration of different protocols and vulnerabilities of SIP VoIP systems have a greater potential for exploitation. Biggest threat to VoIP systems implementation in corporate or military environment at present is unavailability/interruption of service commonly termed as DOS. This research aims at studying and analyzing the VoIP security concerns with specific emphasis on SIP and identifying loopholes in security leading to DOS and on this basis a security framework is proposed to detect and prevent DOS attacks.

Proposed architecture in this thesis involves use of Access Control List (ACL) and CAPTCHA challenge-response mechanism to authenticate users on the network and thus prevent DOS. Simulation of architecture is prepared to test the efficiency and usability of this combination. Analysis of this architecture is discussed in detail to propose and devise a DOS free environment in VoIP systems.

ACKNOWLEDGMENTS

I would thank Almighty ALLAH for giving me strength to finish my studies. I would like to express my gratitude to Brig Imran Rashid for his guidance and support. And finally I would thank my family for their kind support.

TABLE OF CONTENTS

Abstract.....	iv
Acknowledgments	ii
Table of contents.....	iii
List of figures.....	v
List of tables.....	vi
Acronyms.....	vii
1. Introduction	
1.1 Introduction.....	1
1.2 Problem Statement.....	3
1.3 Research Objective	3
1.4 Scope of Research.....	4
1.5 Significance of Research	4
1.6 Research Methodology	4
1.7 Thesis Outline	5
2. Literature Review	
2.1 VoIP Architecture	6
2.2 VoIP Protocol	8
2.3 SIP.....	8
2.4 Handshake model of SIP.....	9
2.5 Security Parameters of SIP	11
2.6 SIP Vulnerabilities	12
2.9 Security Mechanisms	13
3. VoIP Vulnerabilities and Threat Analysis	
3.1 Introduction.....	15
3.2 VoIP Vulnerability Sources	15
3.3 VoIP Attack Vector	17
3.4 Conclusion	21

4. Denial of Service (DOS)	
4.1	Introduction.....22
4.2	Types of DOS Attacks23
4.3	DOS Vulnerability and VoIP Challenges24
4.4	DOS Prevention Techniques.....25
4.5	Conclusion28
5. Proposed DOS Preventive Architecture	
5.1	Introduction.....30
5.2	Usability of Turing Test (CAPTCHA) to Prevent DOS30
5.3	Proposed DOS Preventive Architecture32
5.4	Call Setup / Operational Flow34
5.5	Testbed for Architecture Implementation.....35
5.6	Implementation35
5.7	Discussion / Analysis.....38
6. Conclusion and Future Work	
6.1	Conclusion and Future Work.....41
BIBLIOGRAPHY	44

LIST OF FIGURES

1.1	VoIP Vulnerability Classification.....	2
1.2	VoIP Vulnerability Classification.....	3
2.1	VoIP Architecture Overview	6
2.2	Entities of VoIP Network.....	7
2.3	VoIP Protocols	8
2.4	Finite State Model of SIP Entities Interaction	9
2.5	Three Way Handshake Model Of Sip.....	10
3.1	Call Redirection/ Hijacking	19
4.1	DOS Attack Depiction	22
4.2	Zombies / Botnets	23
4.3	Amplification Attack	23
4.4	VoIP Challenges	24
4.5	VoIP Real Time Sensitivity	24
4.6	Peer to Peer Conversation	25
4.7	Sourcs Monitoring	25
4.8	Destination Monitoring.....	26
4.9	Behaviour Learning	26
4.10	Cookie Verification.....	27
4.11	Re-Authentication	27
5.1	Proposed Architecture.....	32
5.2	Finite State Model of Proposed Architecture.....	34
5.3	Startup of SIP and CAPTCHA Server	35
5.4	Client's Interface.....	36
5.5	Login Received from User.....	37
5.6	CAPTCHA on Client's GUI	38
5.7	Client's Log	38
5.8	Log: State Changed From Setup To Ringing.....	39
5.9	Log: CAPTCHA Challenge	39

LIST OF TABLES

1.1	World Internet Usage and Population Statistics.....	1
2.1	VoIP Layers.....	7
3.1	VoIP Threat Vector.....	18
4.1	Comparison of Audio and other CAPTCHAs.....	40

ACRONYMS

ACL	Access Control List
CAPTCHA	Completely Automated Public Turing Test to Tell Computer and Human Apart
DOS	Denial of Service
DDOS	Distributed Denial of Service
DNS	Domain Name System
HTTP	Hyper Text Transfer Protocol
IPSec	Internet Protocol Security
MGCP	Media Gateway Control Protocol
ITU	International Telecommunication Unit
PSTN	Public Switched Telephone Network
PBX	Private Box Exchange
RTP	Real-time Transfer Protocol
QOS	Quality of Service
SIP	Session Initiation Protocol
SRTP	Secure RTP
SDP	Session Description Protocol
S/MIME	Secure/Multipurpose Internet Mail Extension
TLS	Transport Layer Security
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VoIPSA	VoIP Security Association

INTRODUCTION**1.1 Introduction**

The advent of digital communications have vastly impacted whole world and is the core propellant behind modeling world into a today's global village. Communications have matured from being only voice communications to modern day messaging and video communications. Internet has played a decisive role in expansion and adoption of these technologies into our daily lives. Starting from 1995, today about around 40% of world's population (approx. 3.5 billion) is connected to internet [1]. The ever increasing range of data transmission capability of internet/intranets has helped in bringing the form of ubiquitous computing that we are today seeing in every sphere of our life.

Table 1.1: World Internet Usage and Population Statistics [2]

World Regions	Population (2017 Est.)	Population % of World	Internet Users 31 Mar 2017	Growth 2000-2017	Users % Table
Africa	1,246,504,865	16.6 %	345,676,501	7,557.2%	9.3 %
Asia	4,148,177,672	55.2 %	1,873,856,654	1,539.4%	50.2 %
Europe	822,710,362	10.9 %	636,971,824	506.1%	17.1 %
Latin America / Caribbean	647,604,645	8.6 %	385,919,382	2,035.8%	10.3 %
Middle East	250,327,574	3.3 %	141,931,765	4,220.9%	3.8 %
North America	363,224,006	4.8 %	320,068,243	196.1%	8.6 %
Oceania / Australia	40,479,846	0.5 %	27,549,054	261.5%	0.7 %
World Total	7,519,028,970	100.0 %	3,731,973,423	933.8%	100.0 %

The digital communications have taken a whole new form with the arrival of VoIP technology. This has made communications less expensive, highly flexible and more and more adaptive. Currently VoIP is taking over PSTN (Public Switched Telephone Network) market at a very rapid pace. [3] It is estimated that PSTN networks are losing

an average of 700,000 landline customers per month and there will be 1 billion VoIP users by the end of 2017. It's expected that the VoIP services market will swell 10 percent every year until 2021.

VoIP is a technology that allows standard or IP telephone voice signals to be compressed into data packets for transmission over the Internet or other IP network [4]. VoIP is combination of protocols used for communication of voice signals over IP network. Benefits of VoIP like low cost and flexibility have made it an emerging technology being preferred by corporate and government sectors as a mean of voice and video communication. It offers higher flexibility and more features than traditional telephony (Public Switched Telephone Network (PSTN)) infrastructures, as well as the potential for lower cost and flexibility for consumer market.

Session Initiation Protocol (SIP) is the corner stone of VoIP architecture; on the basis of it entire structure is VoIP communication infrastructure is created. Because of complexities of integration of different protocols and vulnerabilities of SIP VoIP systems have a greater potential for exploitation. All the problems and vulnerabilities of internet are automatically inherited by this technology, as it is mostly based on internet. Even if private intranet is being used, all the vulnerabilities of IP network are inherited. Biggest threat to VoIP systems implementation in corporate or military environment at present is unavailability/interruption of service commonly termed as DOS [5]. As shown in fig 1.1 vulnerability classifications clearly shows major chunk of vulnerabilities is occupied by DOS.

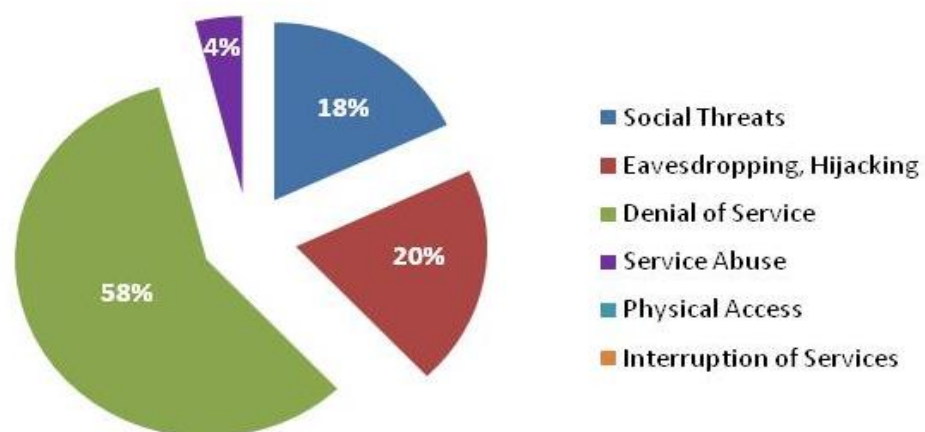


Fig 1.1: VoIP Vulnerability Classification

Fig 1.2 shows that major problem area is implementation rather than protocol or configuration issues [9].

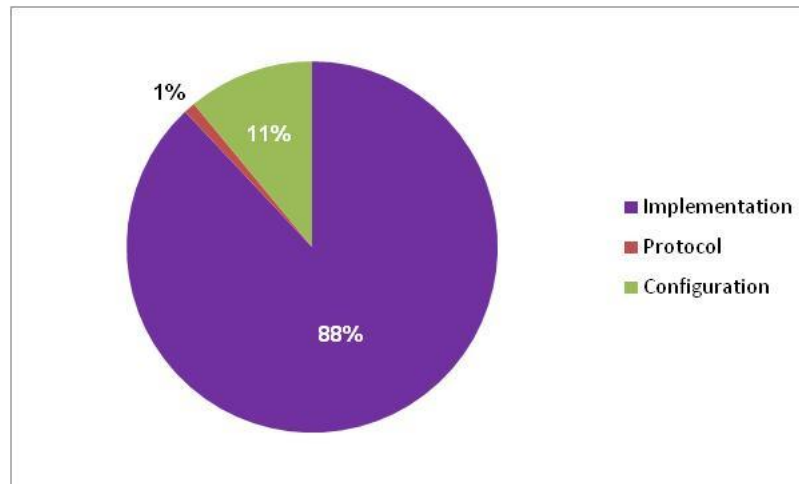


Fig 1.2: VoIP Vulnerability Classification

PSTN has evolved over decades to come up to the level where we are now, in the world of voice communications i.e. when we pick up the phone to call, service is available. [9] If this new technology is to flourish then availability of service is going to be the most important security consideration, which unfortunately is still the biggest hurdle in implementing VoIP instead of PSTN, although both are being used simultaneously in many places for redundancy. According to various surveys, due to inherent vulnerabilities of SIP, DOS is relatively still the most under researched aspect in VoIP security and requires further pondering by researchers [11] [12]

1.2 Problem Statement

Because of complexities of integration of different protocols and vulnerabilities of SIP VoIP systems have a greater potential for exploitation. Biggest threat to VoIP systems implementation in corporate or military environment at present is unavailability/interruption of service commonly termed as DOS [5]. For VoIP communications to flourish, it has to be in par with PSTN service availability level, i.e. when someone picks up IP phone to call, service should be available at all cost.

1.3 Research Objective

The main objectives of this research are: -

- a. Study and analyze the VoIP security concerns with specific emphasis on SIP.
- b. Identify loopholes in security leading to DOS.
- c. Propose a security framework to mitigate security concerns specifically related to DOS attack detection and prevention.

1.4 Scope of Research

The research will mainly focus on studying and identifying SIP vulnerabilities, especially related to DOS, and proposing a high level framework to neutralize the issue. Research will be limited to studying and implementing DOS prevention framework without going into the intricacies of other vulnerabilities of SIP and IP network like confidentiality and quality of service etc.

Complete SIP functionality will be implemented along with other needed functionalities of proposed framework. Simulations have been used to achieve this objective.

1.5 Significance of Research

VoIP is the emerging communication trend in the world, although in Pakistan there are less than 15 VoIP service providers [10]. Because of emerging expansion of mobile communication and internet based communication, VoIP has bright future for expansion in Pakistan. Security issues will be the prime focus when corporate sector will shift toward IP telephony (because of low cost and flexibility). This research will help in resolving availability issues that is the prime concern at the moment and will help in providing framework for secure communications.

The research will assist in grasping the security issues of VoIP especially availability aspect. It will also provide deployable framework to alleviate availability issues in communication. The research will be beneficial for the following areas:

- a. Commercial Sector. The research will assist the industry to understand the challenges of VoIP and improve upon the security aspect of this type of communication. It will also help in improving confidence of corporate sector on VoIP communication services, hence improving the budgetary constraints of industry due to low cost of VoIP.

b. Military. The research will be advantageous for the military as it will provide a secondary communication channel for use in peace and war (although it has the potential to become primary communication channel). It will address security concerns related to VoIP communications as required and envisioned by armed forces.

1.6 Research Methodology

The research will follow simulation method, where a simulation of VoIP network has been prepared using open source SIP implementation available in demo version of Ozeki SIP SDK [21]. It is open source library in .NET environment using c# language. Functionality of CAPTCHA and authentication server has been added and an interface for client is built using C# language integrated using SIP SDK. Complete functionality of SIP will be implemented with added functionality to see the possible effect of text-based CAPTCHA. Results will be used to deduce a working environment parameter of SIP along with CAPTCHA and ACL implementation.

1.7 Thesis Outline

A general overview of how the problem is tackled in this thesis and organization of text is as under.

Chapter 2 reviews the VoIP and SIP functionality and vulnerabilities of SIP-based VoIP services and countermeasures that has been proposed so far in the literature to tackle the security risks in the context of VoIP network.

Chapter 3 reviews VoIP vulnerabilities and threats and the basis of these vulnerabilities.

Chapter 4 reviews DOS vulnerability in general and then its application and problems in VoIP environment.

Chapter 5 introduces a formal concept to tackle DOS vulnerability of SIP based VoIP services. Details of simulation prepared for testing of framework is discussed. Results of simulation have been discussed to present a proof of concept of a DOS free architecture.

Chapter 7 includes future work requirements on the topic and conclusion.

LITERATURE REVIEW

2.1 VoIP Architecture

The main constituents of a general VoIP network are endpoints, SIP servers, authentication servers and PSTN gateway as shown in fig 2 below. The gateway changes over signals from customary PSTN system to VoIP packets and the other way around. Servers gives administration and managerial capacities required for steering of activity, in the vast majority of the cases it is SIP server. IP network is utilized to give connectivity between all terminals. It can be web based internet or private intranet.

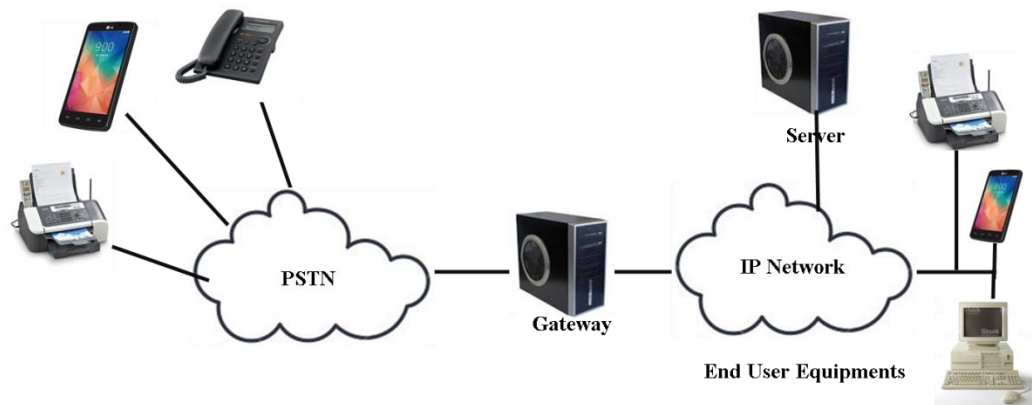


Fig 2.1: VoIP Architecture Overview

VoIP communication system generally consist of front end (soft-phone, PBX, gateway, call manager), back end (CPU, server, storage, memory, network) and intermediate platforms such as VoIP protocols, database, authentication server, web server, operating systems etc. This architecture can be divided into five layers as shown in table 2.1 [6]. Application layer is the client end that hosts softphone, IPPBX and gateways. Infrastructure is basically networking layer that host different networking devices like servers, routers etc. VoIP can be implemented on all platforms like Linux, Windows and Mac, these platforms make up OS layer. VoIP application protocol layer holds the main signaling protocols like SIP and is the major area of our concern. Supporting protocols service layer hold different supporting protocols required by IP network.

Table 2.1: VoIP Layered Architecture

VoIP Application Layer	Softphone, PBX, Voice Mail, Gateway
VoIP Application Protocol Layer	SIP, RTP, RTCP
VoIP supporting Service Layer	(DNS, DHCP, Web, DB, Authentication Server
OS Layer	Linux, Windows, Mac
Infrastructure Layer	CPU, Memory, Storage, Network, Server

VoIP architecture can be further broken down into entities as shown in figure 2.2. Redirect server uses location server to redirect the calls to a particular location, although location proxy and redirect servers can be combined in a single server and may include registrar server also, this depends on the geography, expanse and load capacity/requirement of network

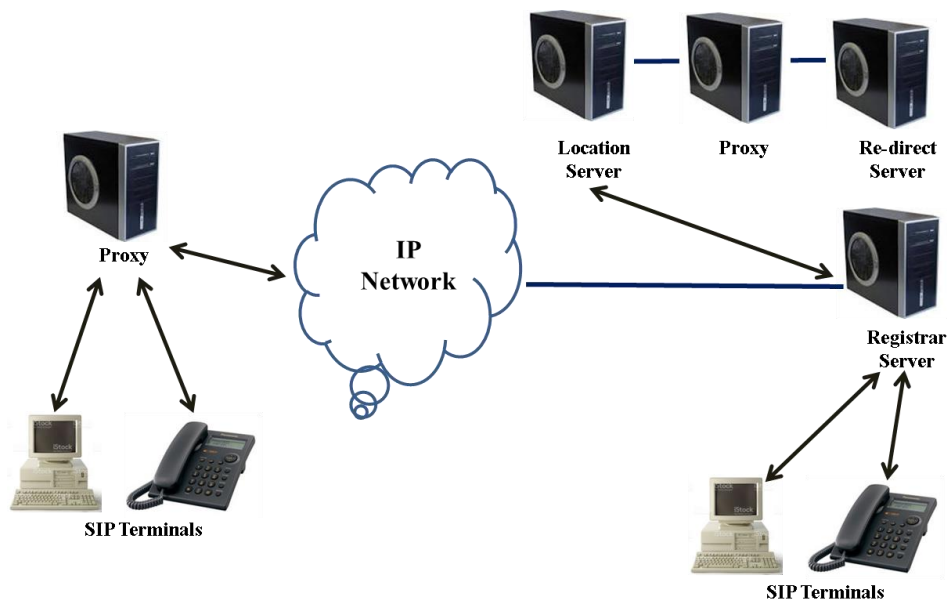


Fig 2.2: Entities of VoIP Network

Location server, redirect and proxy server can be combined as a single entity also, but this will depend on the breadth of network i.e. bigger the network, more will be the processing power requirements of all these entities and they will need to be located separately.

2.2 VoIP Protocols

VoIP necessitates two sets of protocols for communications, first signaling protocols for session establishment and setup and secondly media transfer protocols for transfer

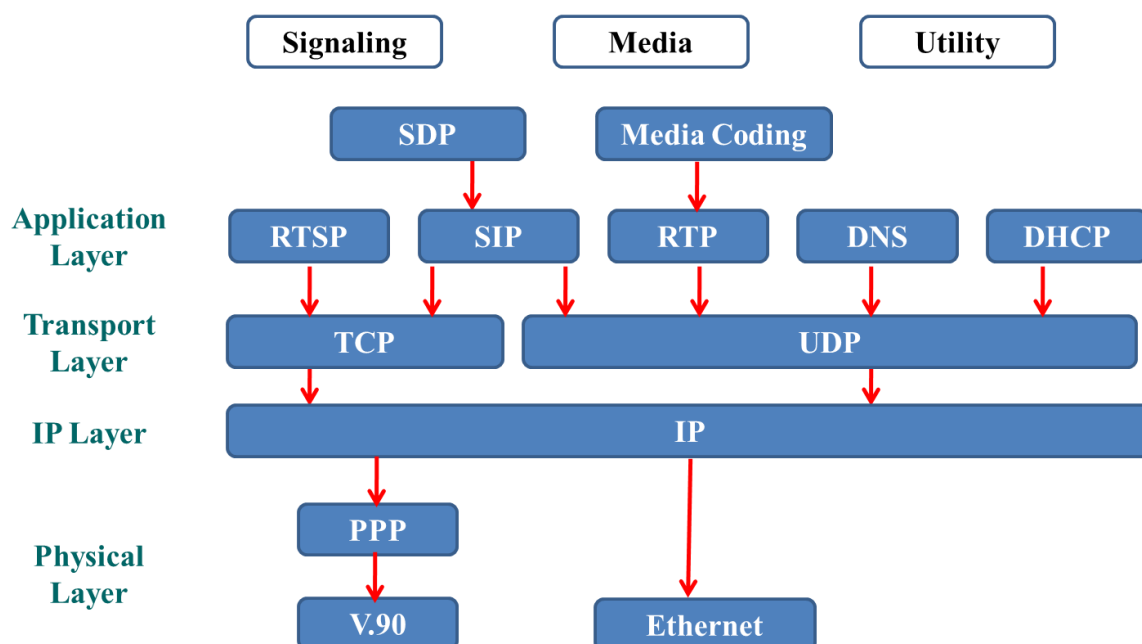


Fig 2.3: VoIP Protocols

of media i.e. voice, video, text etc. Signaling protocols being used worldwide include SIP (standardized by the IETF, RFC 3261), H. 323, MGCP etc. and other patented protocols like skype, CorNet-IP etc. Media transfer protocols like RTP, SRTP, and RTSP etc. Different protocols being used by VoIP are shown in figure 2.3 [7].

2.3 Session Initiation Protocol (SIP)

SIP is an application level protocol used for signaling during VoIP session. It is used for creating, terminating and modifying sessions. VoIP standard session may include telephone calls, video calls and conferencing etc. A new participant can be invited and added to already existing session to make it conference call, likewise, media i.e. video or voice data and existing participants can be added/removed from existing session. SIP uses proxy servers to route requests to the user's current location and performs authentication and authorization. Users can upload current location for use by proxy. SIP works on top of various transport protocols although it is independent of underlying

protocols. Finite state diagram of relationship between different SIP entities is shown in Figure 2.4.

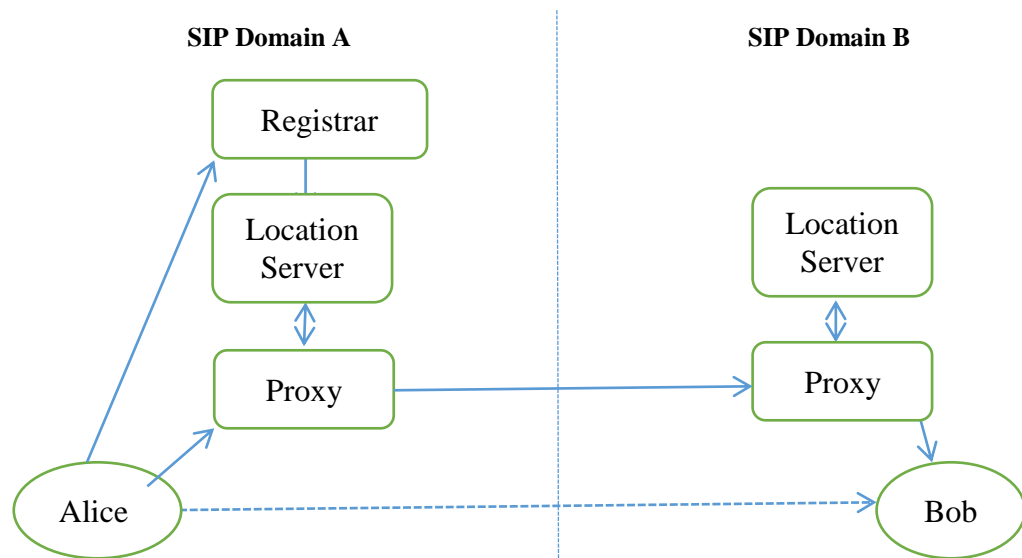


Fig 2.4: Finite State Model of SIP Entity Interaction

Establishing and terminating SIP session is based on five different aspects, these are:

- a. Establishment of session i.e. ringing, establishment of session parameters at caller and called, type of media to be used i.e. video or voice or both.
- b. Location server is used to maintain and find the client being called or recipient of call.
- c. Whether user is capable of participating session i.e. media and processing speed etc.
- d. Willingness of user to participate in the session, i.e. whether user picks up the call or not, it can be termed as user availability.
- e. Management of session includes transfer of session or termination of sessions, modifying session parameters i.e. invoking new services like adding video to a voice session and invoking different services etc.

2.4 Handshake Model of SIP

Uniform Resource Identifier (URI) is used to define a unique identity for all participants or clients. In case of VoIP it is called SIP URI. Format of SIP URI is similar to email such as sip:xyz@domain.com. SIP Secure URI (SIPS URI) option is also available if user want, It will provide transport layer security to transfer of URI, RFC 3261

recommends use of TLS for this purpose. Request and response model followed by SIP is based on HTTP like request and response model.

For establishment of session SIP uses three way handshake model like used in TCP handshake. In figure 2.5 Alice and Bob are two endpoints with two proxies involved in transmission. Session Description Protocol (SDP) is used to include description of caller (caller) and subsequent reply by callee (Bob).

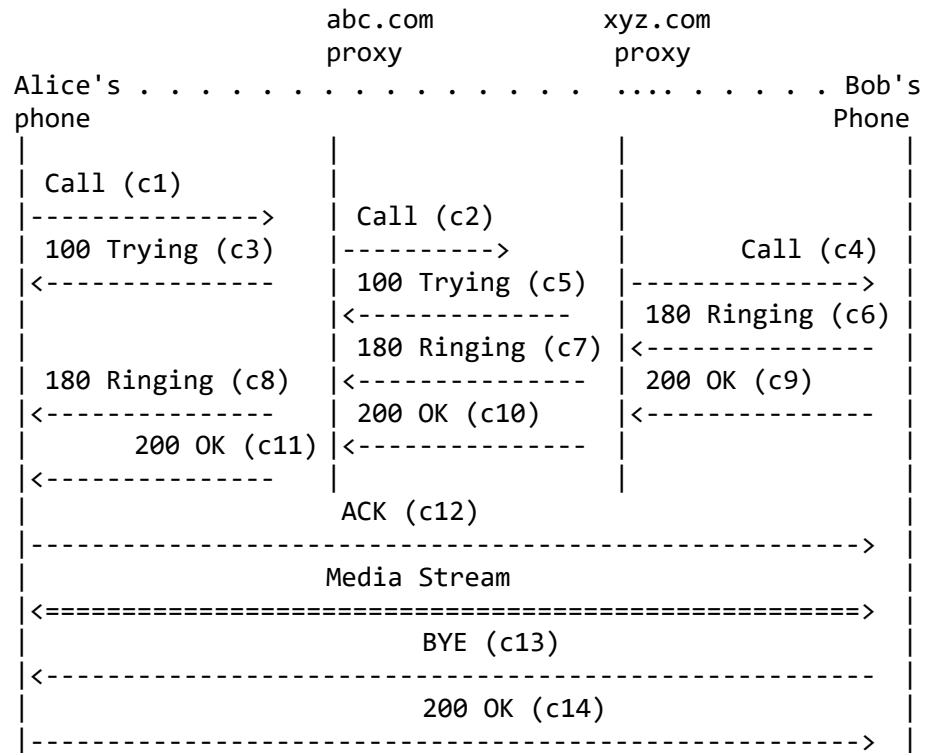


Fig 2.5: Three ways Handshake Model of SIP

Initial call establishment request at Call (c1) from Alice would include URI, Bobs URI or phone number and other details of session. Details of session are not described in SIP, rather body of SIP message contains a description of the session, encoded in some other protocol like SDP. Call is established at ok (c11), it is the point where Bob has picked up the phone line. Now for media transfer media stream takes a different path under different protocols like RTP, SRTP etc. Termination of session would also be directly sent from Alice to Bob or otherwise. However, it depends on the configuration of system and proxies i.e. a proxy may be configured to not allow bypassing in this case when it sends initial call request to nest proxy or destination proxy, it would mention its intentions of remaining present in the session by selecting appropriate header field. [3]

2.5 Security Parameters of SIP

VoIP Networks are subjected to security threats as they utilize public internet as the medium of communication. Since, SIP follows 3-way handshake similar to that of TCP protocol, it is prone to flooding attacks like SYN flooding attack of TCP. Apart from that, there are certain other high impact threats may occur due to breaches in the protocol [8].

a. HTTP Authentication. SIP provides HTTP like challenge based authentication. Digest authentication is used to provide message authentication and replay protection (through nonce). Digest access authentication is one of the agreed upon methods that is used by web server to negotiate credentials like user name & password etc. It applies hash function to credentials before sending them on network. Basic access authentication of SIP uses base 64 encoding instead of encryption, hence non-secure. SSL may be used for security. Although digest authentication does not provide confidentiality or integrity traits of security. It may only be used for authentication.

b. S/MIME (Secure / Multipurpose Internet Mail Extension). S/MIME is a public-private key based encryption algorithm used for signing of MIME data. It provides security of integrity, authentication, and non-repudiation of origin and data security (through encryption). Bodies are signed with private key of sender (public key may be included in message). Bodies are encrypted with public key of intended recipient. S/MIME implementation must have min SHA 1 as digital signing algorithm and 3DES as encryption algorithm. To secure sip header info, S/MIME can encapsulate entire SIP message within MIME bodies of type message/sip and then apply MIME security in same manner as typical sip. Use of S/MIME can create additional overheads also, since; network intermediaries may require examining few header fields for routing the traffic to destination.

c. Security Considerations. SIP is difficult to secure, because of following considerations:

- (1). Usage of intermediaries.
- (2). Multifaceted trust relationship (between different intermediaries like proxies and routers etc.).
- (3). Expected usage between elements having no trust at all.
- (4). User to user operations.

However SMIME and Digest authentication have their limitations. HTTP Digest offers protection of URI and method of message but not to header fields. Next nonce mechanism does not support pipelined requests. Digest is good where UA and servers have pre-existing association but not in case of first use/registration.

Biggest concern with S/MIME is the lack of prevalent public key infrastructure for end user. If self-signed certificates are used, SIP based key exchange is susceptible to man in the middle attack. Keys associated with S/MIME are most useful when associated with user instead of device.

2.6 SIP vulnerabilities

Security considerations mentioned above in 2.5 c amply describe the vulnerability of protocol, which are automatically inculcated in VoIP networks based on SIP; another important aspect is the flexibility requirement of SIP, essential for development and integration with other network protocols. This dictates set of additional security features to be added on deployment. Few threat models based on vulnerabilities of SIP discussed in SIP RFC are as under [3].

- a. Because of absence of any crypto assurance it is possible to modify registration request from any client towards server. It is commonly termed as registration hijacking, and is one of the most potent threats for VoIP service as it can totally compromise the user security. The “From” header field can be modified by the user, so it opens door for registration hijacking.
- b. Integrity of message body cannot be completely ensured since it is possible to hijack session keys from proxy server, as it requires those for routing. Proxy servers will need some header field for routing and those fields cannot be entirely secured in current SIP mechanism, thus violating integrity of message.
- c. Session termination is generally not covered under run down of three way handshake model, session termination request can be sent directly from one user to other without involving proxies and this opens a door for illegitimate termination of a valid session by an attacker who has hijacked few unsecure header fields, that are used for routing.
- d. SIP allows multicast to transmit SIP requests, an attacker can spoof and falsify as a legitimate user of the network and start multicasting false connection

requests. This can result in DOS, which if heightened to DDOS can be very deadly against any network.

2.7 Security Mechanism

Fundamental security requirements for a communication network are as under.

- a. Confidentiality and integrity of message.
- b. Prevent replay attacks/message spoofing.
- c. Authentication and privacy of user.
- d. Preventing DOS.

SIP RFC does not define any new security model; existing SIP security models are derived from HTTP & SMTP. Full encryption of message provides confidentiality of signaling but it is not entirely possible because few header fields are required by proxies to make routing decisions. Low layer security mechanism is required to verify proxies and likewise SIP endpoints needs to be verified. Few techniques which are recommended in RFC are as under:

- a. IPsec: IPsec provides security to network layer. IPsec is not normally used in architecture where a set of hosts or administrative domains have an existing trust. IPsec is usually implemented at OS level in host or on security gateways (as in VPN). When used with SIP, it does not require any integration. Protocols that would be used from IPsec suit would depend on user requirements, so before deployment necessary profiling of tools would be required. RFC does not provide any set of rules in this case.
- b. TLS: TLS provide transport layer security over connection oriented protocols like TCP. TLS is suited for host to host security with no trust association. TLS must be tightly coupled with SIP application. It provides hop to hop security. UA sending request may not know whether TLS is being used end to end. TLS_RSA_WITH_AES_128_CBC_SHA suit must be supported at minimum, when TLS is used.

For high level security UAs authenticate to servers with digest username and password and servers authenticate themselves to UAs one hop away with site certificate of TLS. In peer to peer level UAs trust network to authenticate one another ordinarily, however, S/MIME can be used to provide direct authentication if network is not trust worthy.

For DOS protection TLS & IPsec can be used with hosts/proxies at the edges of administrative domains to bear the brunt of any DOS attack. Stateful proxies are more susceptible to flooding than stateless proxies.

VOIP VULNERABILITIES AND THREAT ANALYSIS

3.1 Introduction

In Mar 2011 a massive DDOS attack hit TelePacific, USA based Telecommunication Company which provides VoIP "Smart Voice" service to thousands of customers [24]. Normally in a month, 34 million SIP traffic registration requests were received at servers of TelePacific, but in Mar 2011 it suddenly shot up to 69 million, resulting in total disruption of services for number of days and caused huge revenue deficit to the company. The offender could not be located as it was ascertained that a huge bot net has been used to launch and camouflage the attacker. This and many such attacks since then pose a huge threat to VoIP based services. These attacks are generally possible because of flexible nature of SIP and ignoring the security considerations and overlooking the vulnerabilities of these systems. Few glaring vulnerabilities, their causes and effects are discussed in this chapter.

3.2 VoIP Vulnerabilities Sources

Software or hardware systems deployed in a network, may it be private or internet, carries some inherent vulnerabilities, which needs to be addressed, to make it efficient. Likewise VoIP also have vulnerabilities which are continuously being exploited. In order to tackle vulnerabilities it is necessary to have knowledge of source or root causes of these vulnerabilities. Few VoIP vulnerabilities sources are discussed below.

- a. VoIP is an IP based network, as the name indicates. It uses internet to traverse the communication flows, so it automatically inherits all the vulnerabilities of web environment like viruses, worms, malicious IP fragments etc.
- b. Since VoIP is mostly based on public network it is prone to all the malicious activities of hackers. An intruder who does not belong to the network may try to disrupt it with malicious or non-malicious intent.
- c. SIP is an open source protocol, so anyone can study it; deploy it for testing or for gaining access to other networks. Because of being open source, attackers can research and identify different vulnerabilities that can be exploited.

- d. VoIP lacks any standard security system, although it supports integration of almost every type of prevalent security mechanism. Inclusion of security mechanisms also increase overheads like extra funds, bandwidth requirements, memory and processing requirements and subsequent QoS issues.
- e. Voice and data integration in same network poses different issues; it increases the management overheads which can be exploited. It requires integration and working of several protocols simultaneously which adds to the vulnerabilities.
- f. Unlike other communication services like mailing and messaging, voice communication requires real time transfer of media, this creates lot of overheads. Inclusion of jitter and noise, even of minor level can affect QoS, further addition of cryptographic means to secure the traffic in route from malicious attacks increase restrain on the network. Because of this reason people using VoIP services, tend to keep security settings to minimum to achieve good quality services, but this phenomenon opens avenues of exploitation to attackers.
- g. Currently deployed VoIP systems mostly use client-server architecture. In these cases clients are mostly located in an open public network. Servers may be secured but open and exposed client may allow attackers to do port scanning and other techniques to find out exposed interfaces receiving calls\ requests and then carry out DOS attacks by generating malicious traffic.
- h. VoIP applications are effected by the type of Operating System they are residing. Different OS vulnerabilities are secured by frequent patches to counter new found vulnerabilities; these patches if not installed on client side may result in exploitation of network.
- i. Deployment of VoIP services require signaling protocols like SIP and media transfer protocols like RTP, Vulnerabilities of these protocols as discussed in previous chapter are automatically induced in every VoIP implementation and need to be addressed before deploying system.
- j. Different VoIP proprietary solutions may have their own coding bugs and errors which coupled with protocol vulnerabilities may affect the entire deployed system.
- k. Media transfer is carried out mostly on UDP, although it can be done over TCP but it can affect quality of media traffic. UDP is a connection-less protocol, it does not validate source IP address, so it is comparatively easy to fiddle with

the integrity of incoming packets. Many IP addresses having forged to a client address can result in reflected DOS attack, due to server responses reflected back to a victim.

l. VoIP traffic flows through switches and routers of the IP network, any compromised system in-between can create serious issues, since routing devices will have full control of routing of packets and many header fields.

m. SIP is responsible for creating and establishing of session. Termination of session does not follow pattern of session establishment rather termination call or BYE may not be traversing through normal checks and proxies. It is sent directly from one client to other, thus terminating the session. This poses a serious vulnerability, an attacker can use zombies to attack a particular victim by spoofing its address and sending BYE signals, it can do this for a long time till tracked or stopped, thus launching DOS. This attack if aimed at more than one victim can result in DOS and jeopardize entire network.

n. HTML plays a major role in web based VoIP communication (e.g. Facebook, Google Hangout), It carries signaling and call setup data in its body. SIP commands are parsed within HTML code and it creates a lot of overhead. Attackers try to inject / execute malicious commands like SQL injection attack, resultantly server authentication can be broken or services can be hung up. Dictionary tests must be performed on HTML code to filter malformed packets that can exploit server. Su and C. Tsai propose two methods to counter this vulnerability [25]. These methods use filtering of malformed packets and chi-square tests to monitor flooding DOS attacks on servers.

o. Phone's caller ID, corresponding MAC and IP addresses are generally stored in call server cache. If attackers can manipulate call server's cache and redirect SIP packets to a specific IP. This can create a lucrative scenario for DOS and DDOS, whereby attacker redirects call to a specific address or addresses. Call servers must be strongly password protected and SIP must be strongly authenticated to prevent such attacks [26].

3.3 VoIP Attack Vector

Vulnerabilities discussed in previous section lead to number of attacks that are possible on VoIP systems, these attacks originate from vulnerabilities discussed above. VoIPSA (VoIP Security Association) is a non-profit organization comprising of VoIP security

vendors and academic organizations [27]. Different classes of threats against VoIP are discussed in VoIPSA threat taxonomy, summary of possible threats is given in table 3.1.

Table 3.1: VOIP Threat Vector

Serial	Main Threats	Subclasses of Threats
1	Social Threats	Misrepresentation
		Theft of Services
		Unwanted Contact
		Harassment
		Extortion
		Unwanted Lawful Content publication
2	Eavesdropping	Call Pattern Tracking
		Traffic Capture
3	Interception and Modification	Call Black Holing
		Call Rerouting
		Conversation Alteration
		Conversation Impersonation and Hijacking
		False Caller Identification
4	Service Abuse	
5	VoIP Specific DoS	Request Flooding
		Malformed Requests and Messages
		QoS Abuse
		Spoofed Messages
		Call Hijacking
		Network Services DoS
		Underlying Operating System/Firmware DoS
6	Other Interruptions of Service	Loss of Power
		Resource Exhaustion
		Performance Latency and Metrics

Attacks against VoIP networks can also be classified as external and internal threats [28]. External threats are in case where attacker is sitting outside the communication network i.e. a normal internet user. Internal threats would be the threats posed by someone who is the legitimate user of network and is thus residing inside the network. External threats can be blocked by using firewalls and other mechanisms but internal threats would be really difficult to defend as attacker's identity would be difficult to ascertain. Few important classes of possible attacks are discussed below.

- a. **Call Redirection.** If a call is intercepted in the midway before reaching its destination, then it would be possible to redirect it to a different path. This can be achieved by registration spoofing i.e. if an attacker can access registration parameters of a certain victim, it can then use this information to redirect the legitimate call to a wrong address, as shown in figure 3.1. Now if this attack is enhanced by using botnet it can result in presenting availability issues i.e. DOS.

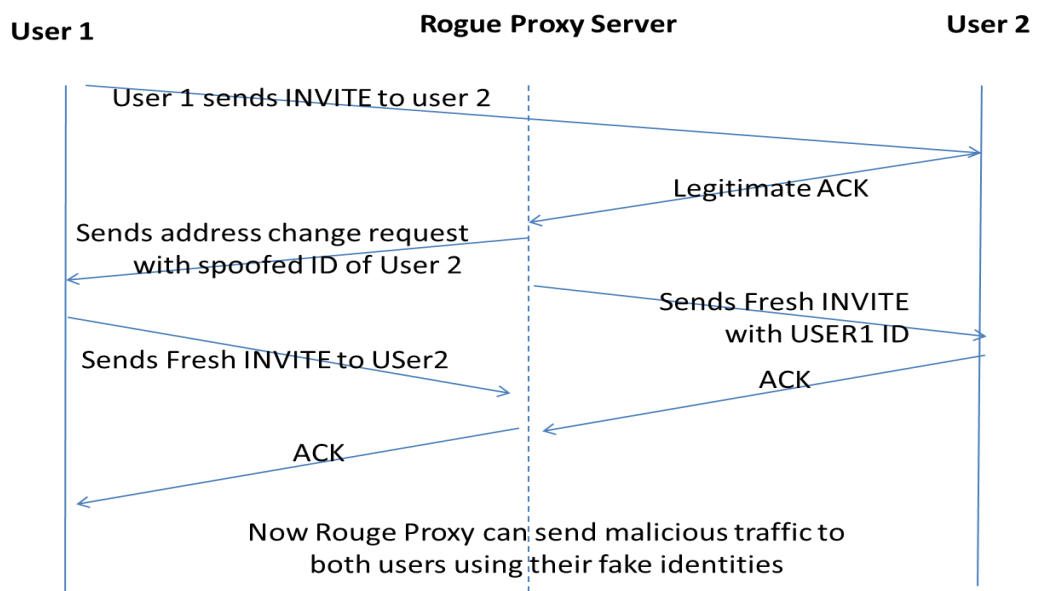


Fig 3.1 : Call Redirection / Hijacking

Fig 3.1 shows how proxy impersonation can be used to achieve call hijacking, in this case rogue proxy server is used to impersonate as a legitimate user and can listen to their conversation or send false messages.

- b. **Registration Hijacking.** VoIP caller use signaling protocol to register itself to the Server or Registrar. Server registers Mac and IP address of client and issues a unique ID or phone number to the client. If this process is hijacked it can entirely jeopardize the system as one individual would be having access to the network through spoofed address and is undetectable if it starts spreading malicious messages or can simply hop into network to listen to compromised client's conversation by redirection attack, explained above [29].
- c. **Service Theft.** Session hijacking or registration hijacking can result into more serious threats when VoIP is being used to provide services such as billing. Unauthorized alteration of billing record can compromise entire systems efficiency. Similarly through network spoofing if someone finds the registration parameters or session parameters, he can simply use any voice or video services for any illegitimate or deadly use like terrorism.
- d. **Interruption of Services.** One of the most serious forms of attack is interruption of services. Interruption of services can result into financial losses as well as interruption of critical services like emergency services. This is the sole and most important reason that VoIP services have yet not reached to a level that these can be implemented on critical emergency services networks. Interruption of services can be un-intentional, like power failure or natural calamity, and these can be intentional also like dedicated DOS attacks to achieve a specific objective, which can be causing financial loss or to create a window to perform any malicious act.
- e. **Malwares.** Malwares can be classified as simple malwares and replicated malwares. Self-replicating malwares are the most dangerous form of worm which can affect entire computer network until stopped. VoIP networks are also susceptible to worms and virus because of all the vulnerabilities discussed above. Spoofed addresses can be used to spread worms through messaging services or even through packet sniffing and modification.
- f. **Weak Security at Endpoints.** Weaker security at endpoints to conserve processing power or memory or due to financial overheads can be very problematic. Weaker endpoints are susceptible to all sorts of attacks and resultantly can compromise entire system. There is a need to ensure correct security classification to be configured during installation of services to prevent attacks.

g. QoS Abuse. An attacker violating the quality of services by adding jitter or noise can hinder the conversations impossible, creating an interruption of services kind of scenario. If session parameters are hijacked packets can be manipulated them by changing the agreed upon codecs during setup.

h. Toll Frauds. Due to wide deployment of VoIP services in corporate sectors, toll fraud cases are becoming a new form of emerging threats. According to a survey toll fraud victims lost around \$4.73 billion in 2013 [30].

3.4 Conclusion

Since VoIP services require integration of various protocols with the major protocol i.e. SIP. This integration creates lots of exploitable vulnerabilities. Quality of Service is the major requirement of VoIP services, because if voice or video quality is compromised then it will render the services useless. This requirement also inculcate vulnerabilities arising from the need to have major portion of traffic bandwidth toward voice and other necessary services, whereas lesser concern is shown toward security considerations. In order to achieve better quality security services are kept to minimum, which exposes the system to attacks, hence, there is requirement to strengthen the endpoints and network with maximum possible protection available.

DENIAL OF SERVICE (DOS)

4.1 Introduction

A Denial of Service Attack is an endeavor to make an asset inaccessible to its expected clients. A standout among the most broadly utilized strategies for DOS is saturating the server/network with extensive number of connection requests that stifles the system bringing about obstructing the legitimate traffic and clients.

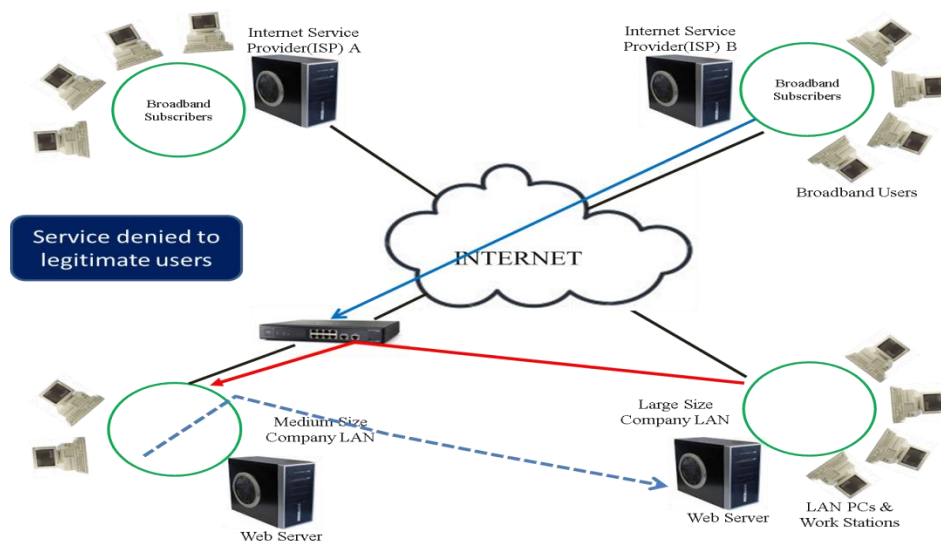


Fig 4.1: DOS Attack Depiction

DDOS (Distributed Denial of Service) is the deadliest form of DOS, where DOS is accomplished by launching assault from various machines. Generally, trading off frameworks are utilized to accomplish it. In most of the cases, compromised systems have no knowledge that they have become part of an attack. DDOS is difficult to negotiate since the originator of the attack is exceptionally hard to follow or trace in a huge internet environment. Compromised systems are called as zombies or botnets [9].

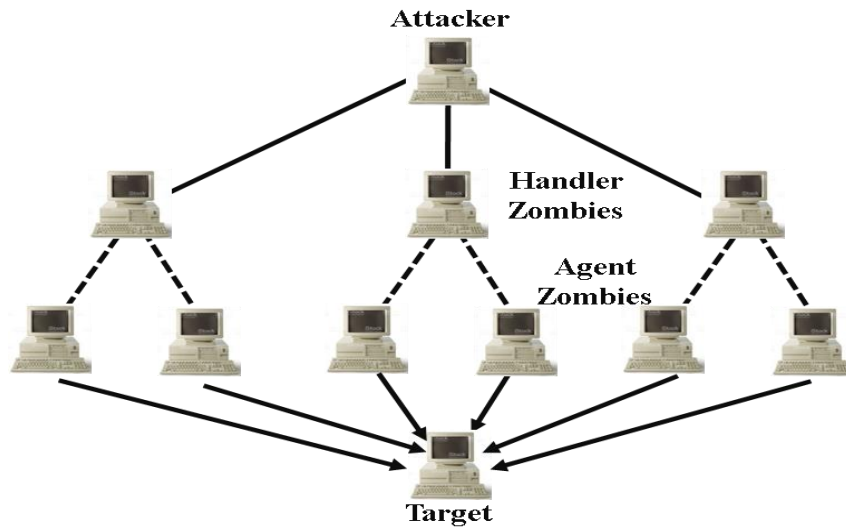


Fig 4.2: Zombies / Botnet

4.2 Types of DOS Attacks

- a. **Reflection** In this type of DDoS attack, attacker spoofs the victims address and sends forged requests to large number of compromised machines (zombies / botnet), and the responses coming back from these machines flood the victim.
- b. **Recursive Amplification attacks** In this attack, attacker sends one spoofed request forging the address of victim i.e. impersonating it as victim and sending it to several compromised or uncompromised machines or servers, which results in multiple requests coming back to the victim and further resulting in even more requests and this keeps on recursing.

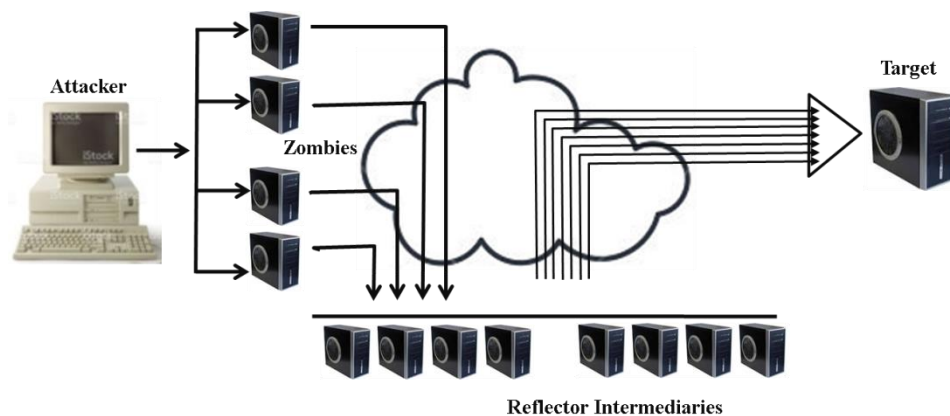


Fig 4.3: Amplification Attack

4.3 DOS vulnerability and VoIP challenges

VoIP is different from other services and applications running over internet because it is a real time critical application, furthermore it is a complex and rich featured protocol with weak endpoints with little or no security. SIP is an application layer session establishment protocol which is open source and has limitations already discussed, which make it more susceptible

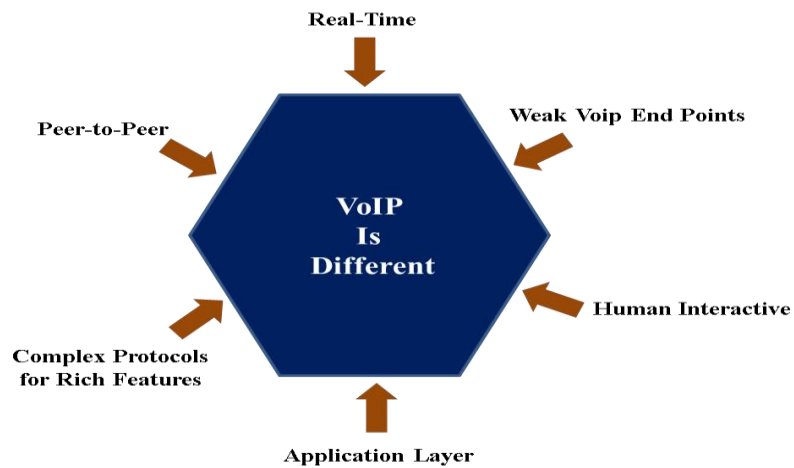


Fig 4.4: VoIP Challenges

Real-time sensitivity of VoIP is a very important factor to be considered while using it, because of involved human interaction. If data packets are lost, out of order or late then person at the endpoint holding mike can't make out the conversation and the purpose of application is lost. Even a two packet 40 ms drop has a perceptible drop in MOS scores. Jitter buffer are usually <100ms a variation in delay of more than that results in drops, ITU specifies 150ms as the maximum end to end delay for voice

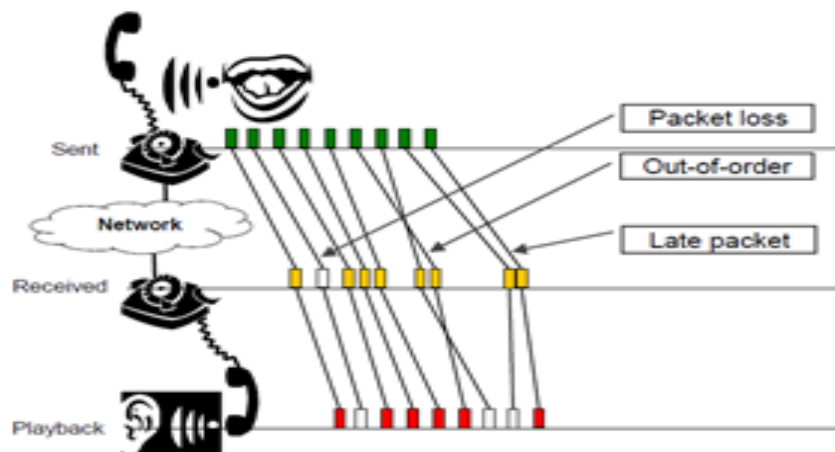


Fig 4.5: Real-time Sensitivity

SIP is the signaling protocol of VoIP, but conversation between endpoints is peer to peer, over UDP, which make it susceptible to attacks. Unlike client server architecture peer to peer has its own vulnerabilities which also form part of VoIP.

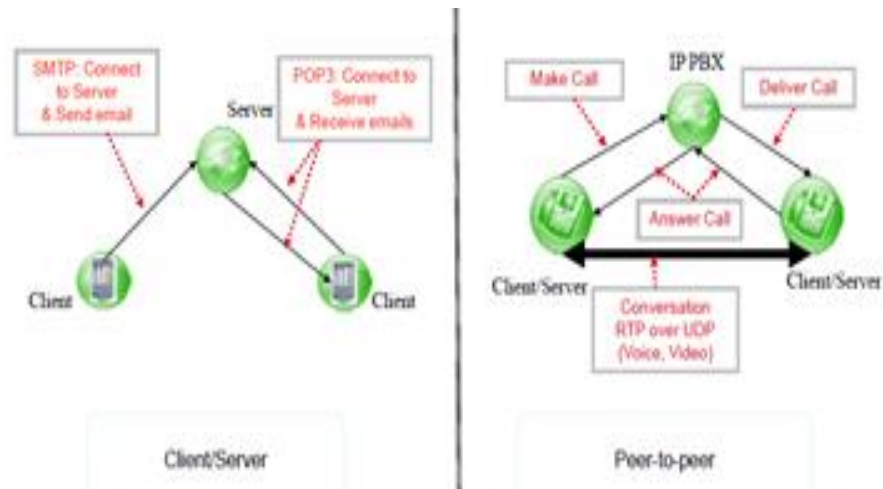


Fig 4.6: Peer to peer conversation

4.4 DOS Prevention Techniques

DOS attacks are recorded since 1997[10], since then, different prevention techniques are being designed, evaluated and taught. IP phones are also susceptible to same DOS attacks as any other application on IP network. Summary of few important techniques is discussed below, in order to evaluate best possible option for VoIP [9].

- a. **Source Monitoring.** Source or originator of traffic is monitored to detect possible DOS attack. Any non-conformant behavior like repeated call establishment requests, or unregistered /unrecognized source is monitored through firewall to block or challenge the intruder.

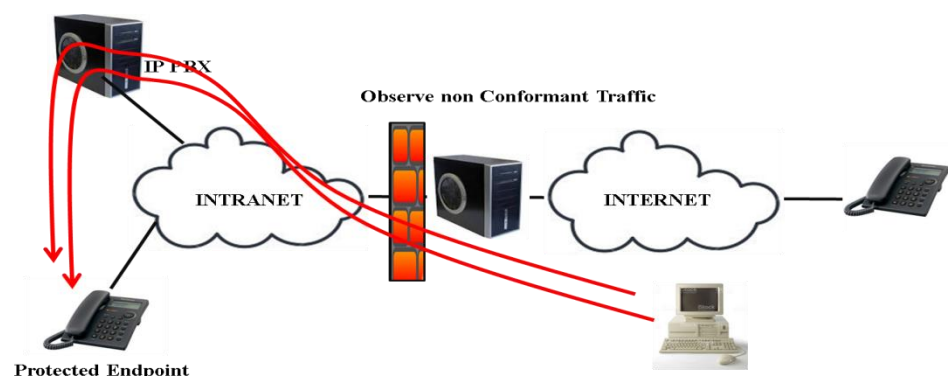


Fig 4.7: Source Monitoring

b. **Destination Monitoring.** Endpoints are protected and monitored to look for any problems like more than permitted amount of traffic coming or pointing toward a protected endpoint. Any nonconforming behavior on a protected endpoint can point toward possible DDOS. This technique is difficult to implement in VoIP environment because of hardware limitations like memory and processing space / speed may not be available.

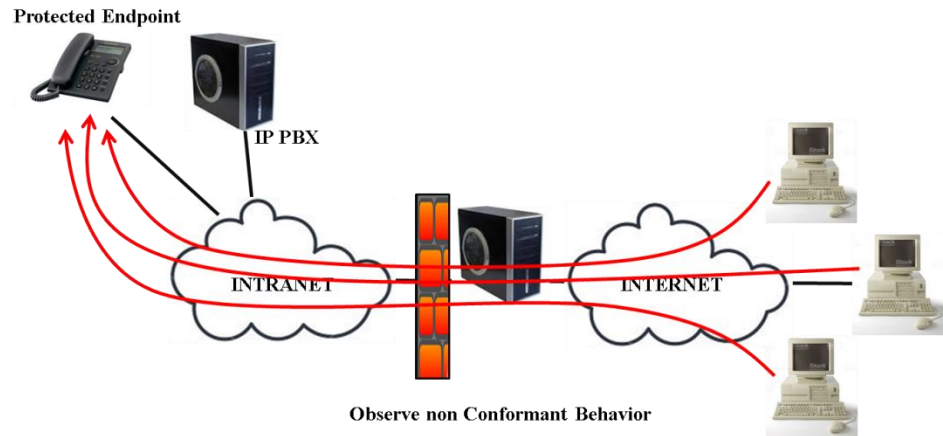


Fig 4.8: Destination Monitoring

c. **Behavior Learning.** Observing the normal traffic patrons on the firewall or proxy to look for any bad behavior, like a single user trying to occupy more space in the network than any other.

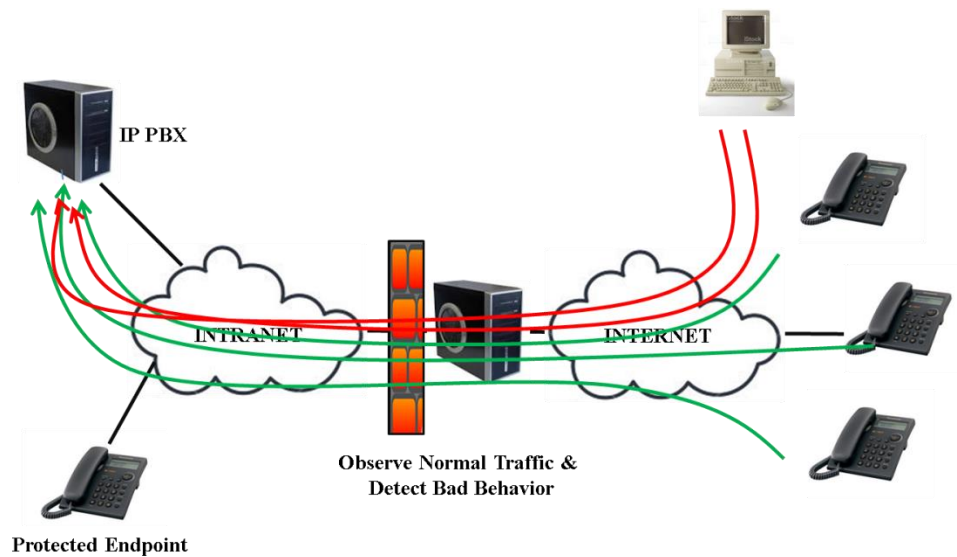


Fig 4.9: Behavior Learning

d. **Cookie Verification.** Another technique to detect DOS / DDOS is through use of cookies. Every time a call is received, challenge response cookie verification request is sent to the caller, if valid response (cookie) is received, only then call is allowed to pass through.

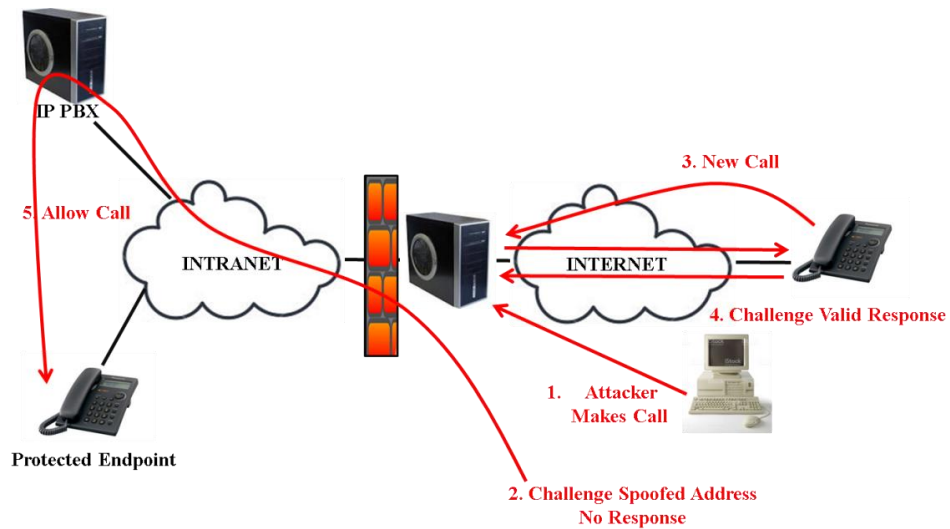


Fig 4.10: Cookie Verification

e. **Re-authentication.** Re-Authentication can be used to detect or block spoofing or zombie attack. This technique is very effective for detecting DDOS, where during call establishment or after specific time of call establishment, caller is required to re-authenticate itself to the server. Re-authentication timer is used by different applications like Facebook. With Facebook Login, your application asks a person to re-enter their Facebook password at any time. You can use this to prevent cases where a user leaves a device logged in or where a third party hijacks someone's session with your application [12].

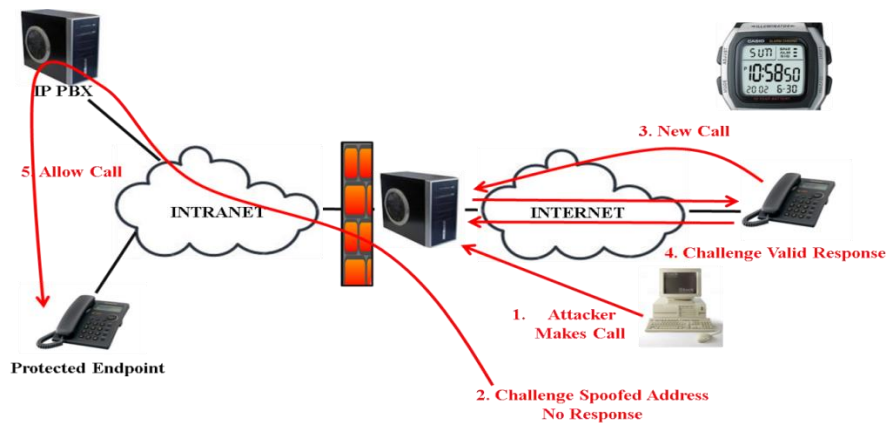


Fig 4.11: Re-authentication

f. Strict Protocol Conformance. Strict conformance with security protocols is very necessary to prevent DOS attacks. Enabling the maximum possible security options available on the device especially in endpoints is necessary to detect and prevent DOS attacks. [9] Weak endpoints are a major vulnerability in VoIP environment, and not allowing the security options available to enhance the performance can result in compromising security.

g. Rate Limiting / Access Control Lists (ACL). Access control Lists (ACL) or firewall channels are the principal line of protection against unwanted access of the network [11]. An ACL specifies which subject is to be granted access or not. For a basic DOS attack coordinated at a solitary client, arrangement of an egress ACL on the client's edge switch or proxy server is a simple approach to stop the attack. The issue with ACL is scaling both from a router side and as the attack vector increases. Implementing ACLs must be in line with the hardware restrictions on which they have to run.

ACL maintains record of clients or group of clients profiling information and their access rights in a particular architecture or framework. Information is stored in database and is used to match and give access rights to all the visiting clients. These clients' and groups with their rights are categorized as entities of ACL. These entities are known as access-control entities (ACEs), in Microsoft Windows framework [13]. Each available query contains an identifier to its ACL. The benefits or consents decide particular access rights, for example, regardless of whether a client can read from, write to, or execute a question. ACLs are also categorized as file system and networking ACLs

Proprietary hardware ACLs are also used on routers or firewalls. These ACLs provide rules that are applied to port numbers and IP addresses. Individual servers as well as routers can have network ACLs. Access control lists can have separate rules for inbound and outbound traffic. All ACL entries are read from top to bottom i.e. top down approach is used, as soon as matching entry is found search is stopped and valid rights are granted.

4.5 Conclusion. Monitoring and Filtering: like Web and mail servers, SIP intermediaries and proxies need to keep up monitoring of suspicious clients and deny those clients from setting up sessions. These rundowns can be built up by checking the transactions served by the proxy intermediary, also, logging client behavior (e.g., clients that reason a sudden increment in the quantity of served transactions or clients included in unfinished setups).

Authentication is another approach which can help in preventing unauthenticated client from entering into the network, but this would be true if it is assumed that attacked is not spoofing the identity of a legitimate user. SIP uses digest authentication like HTTP [8], which requires maintenance of state at server, this is done by storing the issued challenge. This can be misused by breaking unfinished session i.e. if attacker ignores or sends false response and starts another session. Answer to this, problem can be use of predictive nonces [22]. Nonce is calculated in a way that makes them valid only for a certain time window for validated messages. When a response arrives at a server, the nonce is first verified to be correct, followed by the verification of the response. This method can works without any changes to the protocol.

An undeniable defensive measure for diminishing the danger of memory weariness attacks is use of stateless proxies to execute as much server usefulness in stateless mode before going stateful. The stateless hindrance ought to be utilized to execute the same number of security checks as would be prudent, including stateless validation of clients, checks of unapproved outsider enlistments, or separating of surely understood spam sources.

Keeping in mind the end goal to abstain from blocking approaching messages while the server is caught up with handling a message or while sitting tight for an answer from an outside server a SIP proxy ought to be actualized utilizing strings or parallel forms with each procedure or string in charge of preparing one message at any given moment. Here a center part just goes about as a message scheduler dispersing approaching messages between the procedures. Each procedure is then in charge of parsing the message, starting any DNS request or asking for the execution of an application, lastly sending the message.

PROPOSED DOS PREVENTIVE ARCHITECTURE

5.1 Introduction

In this chapter we will discuss a proposed architecture to implement DOS resistant VoIP applications. The security issue of SIP based services winds up plainly evident with the expansion of the fame of these services. In spite of the fact that mixes of solid access control and encryption strategies can be a decent way to deal with secure attacks against SIP based administrations, guaranteeing these approaches is not really versatile in the exceptionally open and dynamic design of the Internet. The IETF has made a few changes that give insurance to the VoIP signaling and media streams. Because of the overheads of usage and execution these security systems have not been completely actualized and conveyed in current VoIP applications. Additionally, existing security arrangements are not efficient to adapt to the expanding modern huge scale assaults and malwares circumstances in SIP based administrations. Therefore, Intrusion Detection System (IDS) have turned into a crucial segment of security infra-structure to recognize interruption or atypical conduct that passes the current security policies.

5.2 Usability of Turing Test (CAPTCHA) to Prevent DOS

Turing Test is used to detect any abnormal behavior of participating entities by presenting challenge-Response CAPTCHA. [16]A CAPTCHA is a strategy that is broadly used to counter mechanized SPAM assaults. A similar strategy can be utilized to relieve SPIT. A CAPTCHA is a Reverse Turing Test where a machine tries to distinguish whether the approaching session is started by a product application or a human. The three noteworthy classifications of CAPTCHA are visual CAPTCHA, where the client tries to perceive characters or words in distorted pictures, audio CAPTCHA, where the characters or words to be perceived are in a sound record, and rationale CAPTCHA, where user tries to answer a specific question.

Researchers have used CAPTCHA technique in various researches, although a survey conducted on the research publications of VoIP could identify only 4 publications out of 245 reviewed publications [4]. Quittek et al. [14] propose the utilization of concealed Turing tests to distinguish SPIT guests. As a solid approach, they use the association

display in human discussion, which limits the measure of concurrent ("twofold") talk by the members, also, the way that there is a short delay toward the start of an addressed call, trailed by an announcement by the callee that starts the discussion. By searching for indications of infringement of such standards, it is conceivable to recognize naive computerized SPIT guests. The authors actualize their plan and coordinate it with a VoIP firewall. Wang [15] portrays an end-point audio CAPTCHA framework for countering SPIT, intended to be introduced and utilized by clients also, administrators. Usability study conducted by her, points out the establishment and administrative overheads in implementing audio CAPTCHA, for users who can understand English language.

Both types of CAPTCHA i.e. audio and image / text based can be applied in VoIP architecture, although major work has been done in the field of audio CAPTCHA association in VoIP architecture. Both types are discussed as under:

- a. **Audio CAPTCHA** Existing sound CAPTCHAs are demonstrated more hard to use for visually impaired than visually non-impaired individuals. [17] A research pointed out that just 43% of clients with visual disabilities could reply an audio CAPTCHA at the first endeavor. In addition, it ought to be noticed that visually impaired clients took time no less than twice as long as other users. However about half of clients (47%) neglected to react accurately to a audio CAPTCHA after 3 endeavors. This is to some degree unforeseen outcome, since one would expect that audio CAPTCHA difficulties would be more fitting for people with eyesight problem.

Y. Soupionis and D. Gritzalis (Soupionis and Gritzalis, 2010) characterized the audio CAPTCHA qualities, assessed the current prevalent sound CAPTCHA usage [18]. The assessment procedure depended on the way that CAPTCHAs must be simple for human clients to settle, simple for an analyzer machine to create and grade, and hard for a product bot to settle. In this manner, 60 clients and two bots were used to handle CAPTCHA. The assessment procedure demonstrated that a) the current CAPTCHA usage are not satisfactory, implying that each execution is either as well simple or too hard to be in any way illuminated by the two clients and bots, and b) the usage qualities of some CAPTCHAs, as long vocabulary (> 8 characters) and dialect prerequisites (local

versus non-local English speakers), influences contrarily the clients' achievement rate (~40%) by and large.

b. **Text Based / Image CAPTCHA** Generally text-based CAPTCHA that are in use are basically a picture design that contains alphanumeric characters that is placed in front and background is distorted in way that it is difficult for OCR (Optical Character Recognition) softwares to recognize the characters but at the same time should be easily handled by human. A decent quality CAPTCHA is to be robust and secure. Different types of CAPTCHAs have been implemented and are being used in web environment; these can be object identification, text recognition, puzzle solver etc. Text based CAPTCHAs are mostly used because of easy implementation and low cost [19].

OCR softwares are used to break text-based CAPTCHAs. Character recognition (OCR) is used to break text-based CAPTCHA. OCRs generally segment the image into different small parts, as small as a single character and then try to recognize the character. CAPTCHA systems usually distort the image in a way that makes it more complicated for OCRs to pick up all the characters. As the OCR attacks are getting stronger there is need to strengthen the text-based captcha so noise is added by using colored backgrounds and use of various shapes like lines, thick lines, rectangles, ovals and circles etc.

5.3 Proposed DOS preventive Architecture

DOS attacks are seldom conducted by a single user, generally botnet or zombies are used to launch such attack. Our proposed architecture relies on use of image CAPTCHA coupled with Access Control List, which is to be maintained by authentication servers, that to detect any possible DDOS attack (Fig 5.1).

Three main entities are used to demonstrate the impact of CAPTCHA in real time, these are authentication server, CAPTCHA server and endpoint that have an interface to accept and reply to challenge. Role of these entities is discussed under:

a. **Proxy Server** Proxy server is used here as SIP server, which implements the basic functionality of VoIP / SIP. This server will have following properties:

- (1) Can send / receive call setup request to/from Authentication server

- (2) Can only send and receive multimedia streams, if a caller in the intranet has a pending call setup request and has a valid authentication certificate assigned to it by the authentication server.
- (3) Should handle call setup requests from within local intranet without involving authentication server.

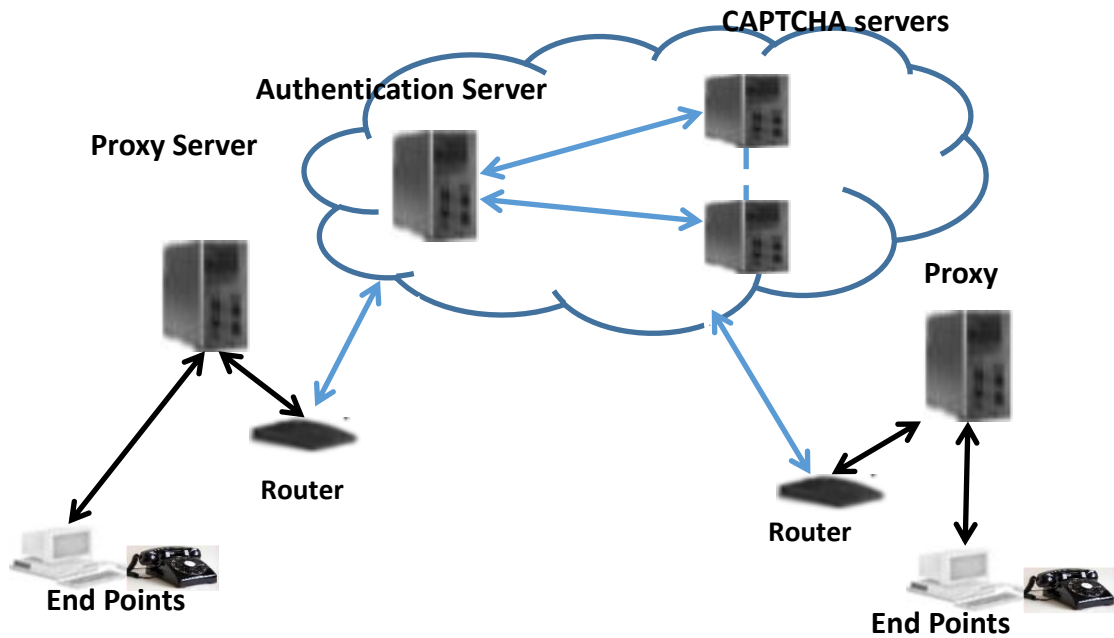


Fig 5.1: Proposed Architecture

b. **Authentication Server** Authentication server is used to authenticate the incoming call through lookup table of ACL and will also communicate with CAPTCHA server to fetch and check challenge-response from server and client.

- (1) Can receive call setup requests passed from a Proxy server
- (2) Maintains ACL to control source monitoring based on following rules.
- (3) Previously authenticated caller's call request is automatically forwarded without involving CAPTCHA servers.
- (4) Call requests from new caller is passed on to CAPTCHA servers for verification.

- (5) Call request from caller whose ack from called endpoint is pending.
 - (6) Call requests having certificate of authentication from other authentication server in intranet.
 - (7) Will always forward call requests to called endpoint after attaching authentication certificate.
 - (8) Will control congestion by having a check on traffic volume to a specific proxy server depending on its bandwidth.
- c. **CAPTCHA Server** These servers are used to generate and check image CAPTCHA received from client
- (1) Presenting CAPTCHA to authentication server on request
 - (2) Validating response of CAPTCHA from authentication server.
 - (3) Forwarding result of CAPTCHA challenge / response to authentication server.

5.4 Call Setup / Operational Flow

Basic concept of this proposed architecture is to establish a DOS free communication mechanism i.e. ensuring availability requirement of security matrix. Confidentiality or integrity of voice communication can be ensured through encryption and public private keying mechanisms, although these factors are not discussed here, we restrict ourselves to availability for the purpose of this thesis.

Any incoming call will be categorized as white, black and grey by authentication server. Previously authenticated users will be whit listed in ACL implemented on authentication server and black listed will be those callers who have not been able to register successfully or failed CAPTCHA challenge three times, previously. Grey is the new caller who is new on the network and will be presented CAPTCHA challenge to solve, on successful completion of challenge-response, call will be allowed to setup by proxy server and the client will be added in white list or otherwise. Finite state diagram of this architecture is given in Figure 5.2

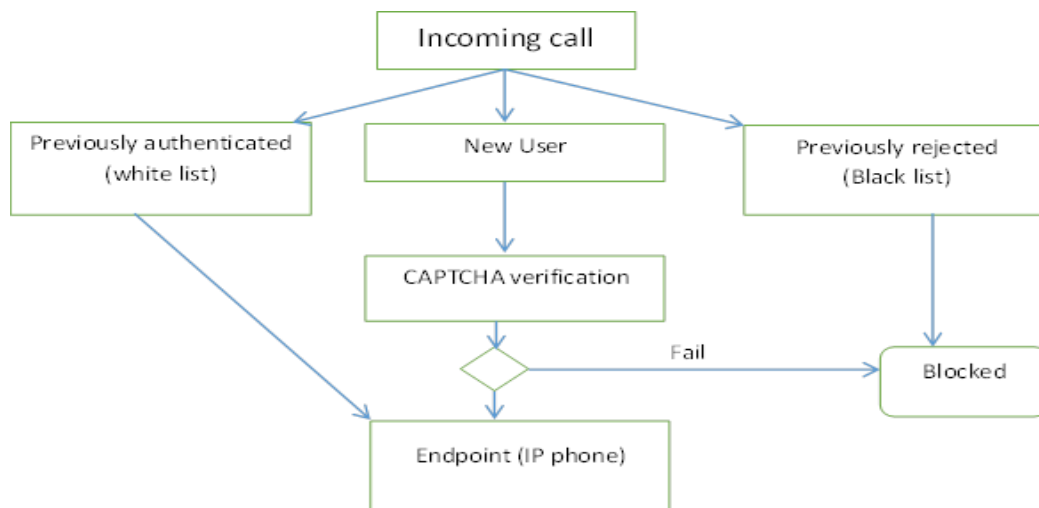


Fig 5.2: Finite state model of proposed architecture

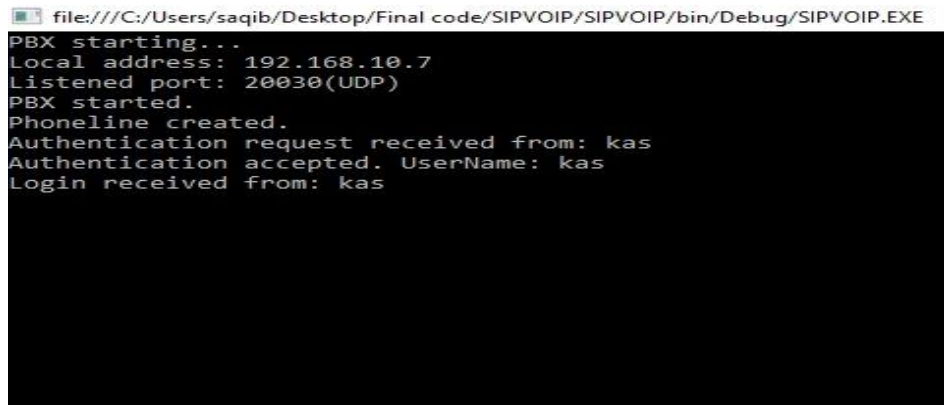
ACLs are generally employed in network as a filter to parse the incoming traffic by checking its legitimacy and other parameters as defined in ACL. We have put ACL in authentication server to authenticate the incoming traffic and generate valid challenge-response mechanism.

5.5 Testbed for architecture implementation. We tested our proposed architecture by deploying a fully configured SIP server with addition of authentication mechanism and a CAPTCHA server to implement text-based CAPTCHA. Testing has been done in .NET environment using C# language. Ozeki Informatics Ltd is a Hungarian company that provides communication products throughout the world. For our test we have used open source demo version of Ozeki SIP server which is implemented in c# library that can be used in .NET environment. It gives full SIP implementation, which has been used to integrate ACLs and CAPTCHA server. For testing purpose we have used one computer system Core i5, for implementing SIP server, authentication server and CAPTCHA server. Two other computer systems are used as softphones/clients, having SIP client functionality. Front end for calling and receiving is designed in C# and is integrated with client and servers.

A PBX (Private Branch Exchange) establishes communication line with in an enterprise or organization. It is used for switching telephone calls within an enterprise, keeping an interface for outbound and incoming calls and managing internal switching of calls. The end points attached to SIP accounts are called extensions of the PBX.

5.6 Implementation

General requirements for implementation are Ozeki SIP SDK installed on three PCs, one for server implementation and two for client or softphone role. Coding is done in C# using Ozeki VoIP SDK library. SDK is installed on client side with client code only. CAPTCHA and ACL services are also imbedded in SIP server. Front end for client side is designed using C# and integrated with client code.



```
file:///C:/Users/saqib/Desktop/Final code/SIPVOIP/SIPVOIP/bin/Debug/SIPVOIP.EXE
PBX starting...
Local address: 192.168.10.7
Listened port: 20030(UDP)
PBX started.
Phoneline created.
Authentication request received from: kas
Authentication accepted. UserName: kas
Login received from: kas
```

Fig 5.3: Startup of SIP Server and CAPTCHA Server

To look up server status command line interface is used. Logs are maintained to log all the events with timing i.e. registration request, registration status, call setup request, call status etc. Logs will help evaluate the time requirement of call setup without and with CAPTCHA services invoked.

When server is started it will operate on local IP, or IP can be assigned also and port number is also already assigned. Figure 5.3 shows the startup of server as seen on command line interface. CAPTCHA server module is automatically started with start of server. Here “KAS” is the acronym used for CAPTCHA server.

Client interface is shown in figure 5.4. On Startup client is required to login with authentication server. Client side code works and communicates with server on the

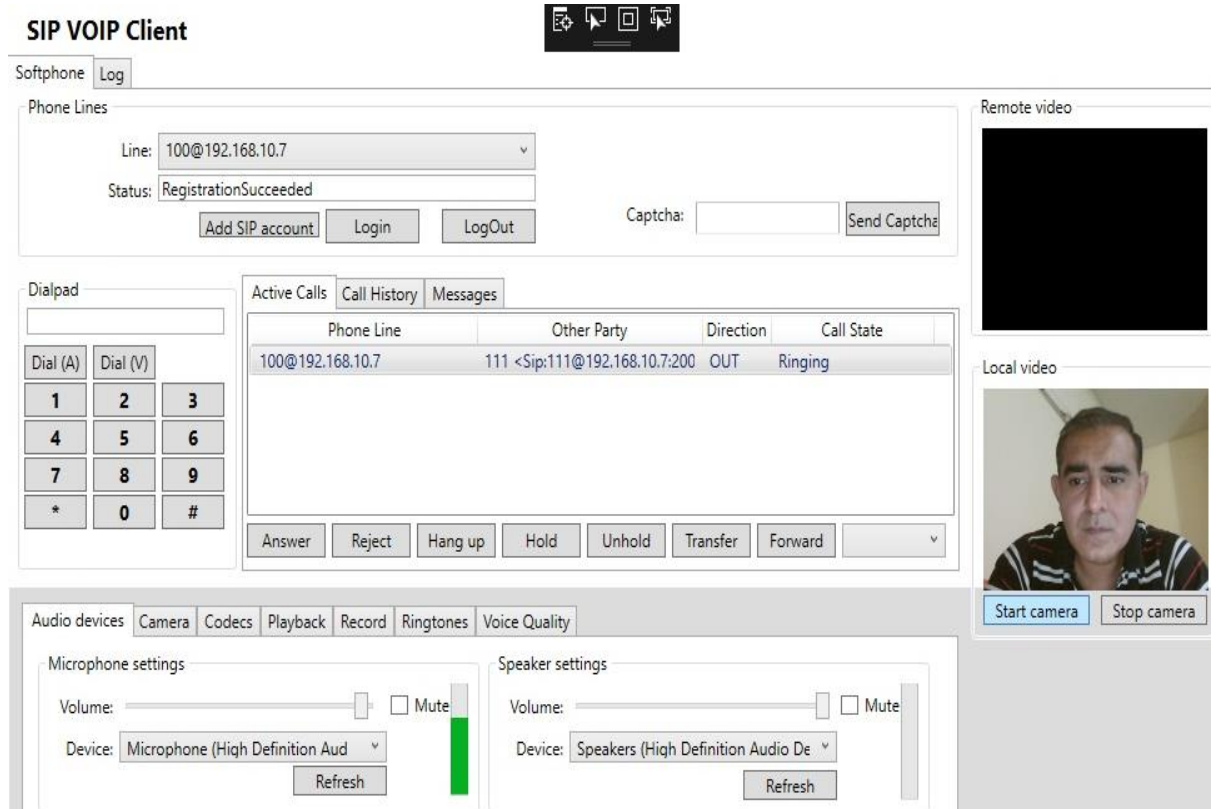


Fig: 5.4 Client's Interface

designated IP and port number, in this case on IP 192.168.10.7 and port number 20030. Command line interface shown in figure 5.5 shows the login steps of client having phone number 111. Authentication request is automatically accepted, if client is already registered with authentication server and has valid permission in ACL.

```

file:///C:/Users/saqib/Desktop/Final code/SIPVOIP/SIPVOIP/bin/Debug/SIPVOIP.EXE
PBX starting...
Local address: 192.168.10.7
Listened port: 20030(UDP)
PBX started.
Phoneline created.
Authentication request received from: kas
Authentication accepted. UserName: kas
Login received from: kas
Authentication request received from: 111
Authentication accepted. UserName: 111
Login received from: 111

```

Fig 5.5: Login Received From User

After successful registration client can make calls. ACL is automatically maintained to record the status of each client, which can be white, Grey or black. White is the legitimate client who is already known to the authentication server, call from such client will be automatically processed without invoking CAPTCHA services. Screen shot of client side user interface is shown in figure 5.4. It provides client the functionality of login, dialing and receiving audio or video call, sending and receiving text messages and viewing current call status. It also maintains call history that can be viewed by client.

GUID (Global Unique identifier) is the key that is used to create image presented as CAPTCHA. .NET has inbuilt GUID generator, that is used to generate six figure mixed characters (upper and lower case mixed) and numerals. CAPTCHA is presented on top right corner of client interface, as shown in figure 5.6.

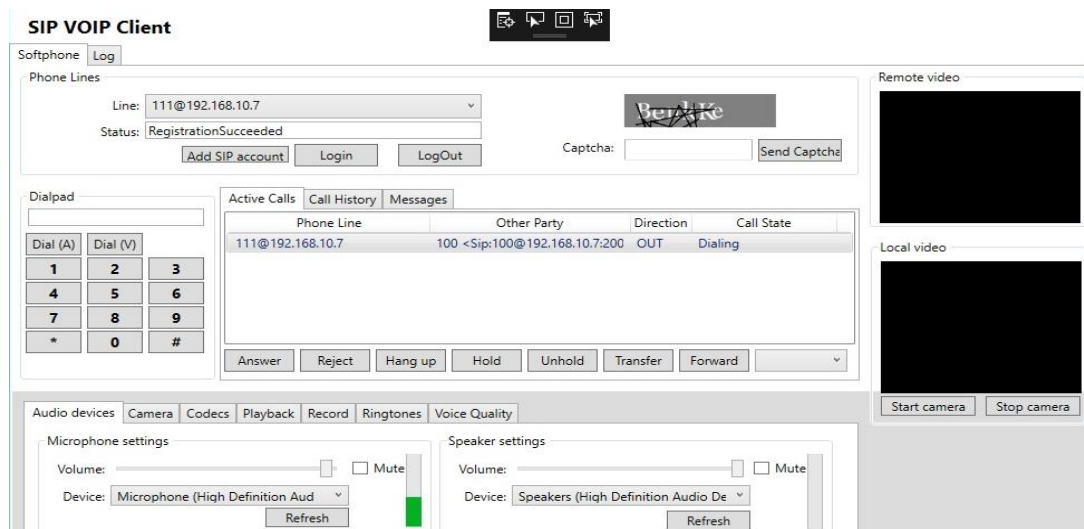


Fig 5.6: CAPTCHA on Client's GUI

Logs are automatically maintained on server and client side, screenshot of log is shown in figure 5.7. Logs are maintained to view and analyze time spent in call setup at different stages. Following events are logged.

- a. Login time of client
- b. Registration successful time
- c. Call setup request
- d. CAPTCHA sent
- e. Valid CAPTCHA received
- f. State changed to ringing
- g. State changed to answered

- h. State changed to completed
- i. Closing call
- j. Client logged out

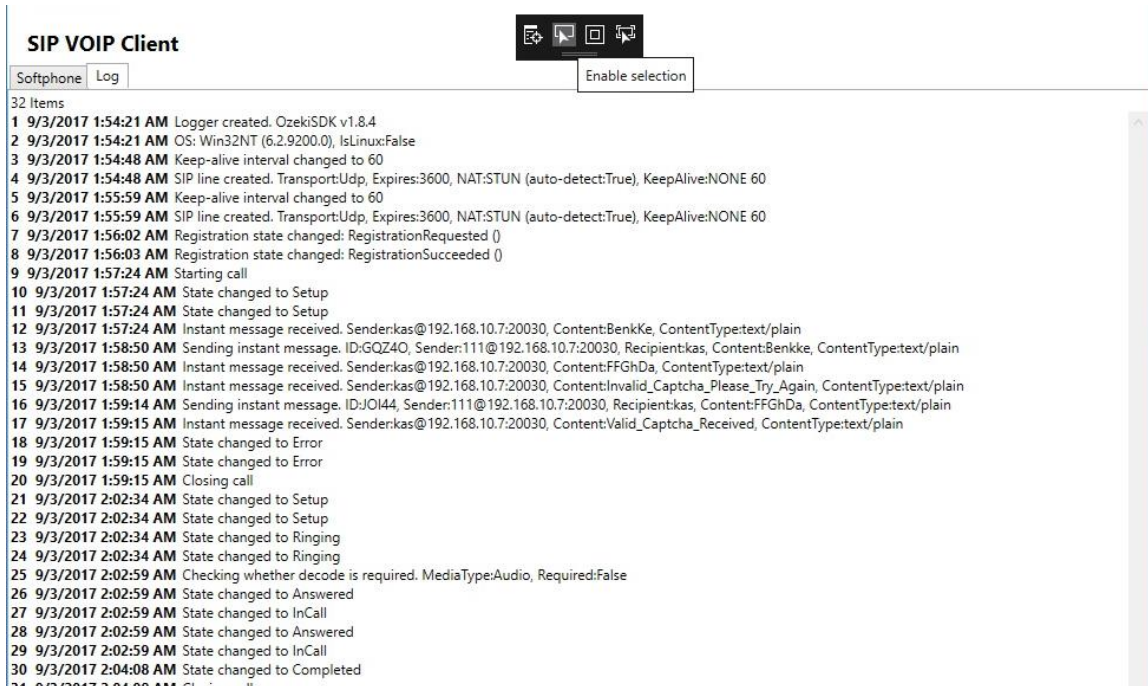


Fig 5.7: Client Log

5.7 Discussion / Analysis.

Analysis of logs will demonstrate the time required to solve the CAPTCHA challenge and the total call setup time. Portion of log is shown below in figure 5.8. Time spent in solving the CAPTCHA challenge in this case is 11 second (12:15:30-12:15:41), whereas, total call setup time is 12 sec.

```

67 9/4/2017 12:15:29 AM Starting call
68 9/4/2017 12:15:29 AM State changed to Setup
69 9/4/2017 12:15:29 AM State changed to Setup
70 9/4/2017 12:15:30 AM Instant message received. Sender:kas@192.168.10.7:20030, Content:8F6Qvh, ContentType:text/plain
71 9/4/2017 12:15:41 AM Sending instant message. ID:1C7VUy, Sender:111@192.168.10.7:20030, Recipient:kas, Content:8F6Qvh, ContentType:text/plain
72 9/4/2017 12:15:41 AM Instant message received. Sender:kas@192.168.10.7:20030, Content:Valid_Captcha_Received, ContentType:text/plain
73 9/4/2017 12:15:41 AM State changed to Ringing

```

Fig 5.8: Log- State Change from Setup to Ringing

This setup time generally doubles and triples in case of wrong solution of CAPTCHA twice or thrice. After 3rd challenge is unsuccessful, caller is black listed, and won't be permitted to call on this network.

```

21 9/4/2017 12:10:15 AM Starting call
22 9/4/2017 12:10:15 AM State changed to Setup
23 9/4/2017 12:10:15 AM State changed to Setup
24 9/4/2017 12:10:15 AM Instant message received. Sender:kas@192.168.10.7:20030, Content:8F6Qvh, ContentType:text/plain
25 9/4/2017 12:10:30 AM Sending instant message. ID:J3zFO, Sender:111@192.168.10.7:20030, Recipient:kas, Content:8F6Qvh, ContentType:text/plain
26 9/4/2017 12:10:30 AM Instant message received. Sender:kas@192.168.10.7:20030, Content:Valid_Captcha_Received, ContentType:text/plain
27 9/4/2017 12:10:31 AM State changed to Ringing

```

Fig 5.9: Log-CAPTCHA Challenge

In case of figure 5.9, challenge is solved in 15 seconds. Average time to complete CAPTCHA challenge was found between 10-15 seconds and average call setup time from start of call till ringing (with CAPTCHA challenge involved) is 11-16 seconds, although this time will vary with different age group and having people with eyesight problems and few other factors.

Audio CAPTCHA takes much longer in creation phase. [20]The overall time spent in creating full set of 3-digit CAPTCHA takes 8 sec, whereas creating a 4-digit CAPTCHA takes 107 sec. Although implementations can be made efficient but in general it requires more processing time to present audio CAPTCHA and is even more difficult to solve it because of addition of noise and jitter of speech, speech quality also matters a lot in this case.

Table 3.1: Comparison of Audio and other CAPTCHAs

	Audio CAPTCHA	Text CAPTCHA
The overall time spent in creating 3-digit CAPTCHA	8 sec	<1 sec
Creating a 4-digit CAPTCHA	107 sec	<1 sec
CAPTCHA solving time	>25 sec	10-15 sec
Effect of Noise / Jitter	Decrease success rate	No effect
Vocabulary / Language differences	Decrease success rate	No effect
Anomaly CAPTCHA response time is 42 seconds with 90% accuracy		

Through this simulation, we can reach to the conclusion that text based CAPTCHAs are easy to handle and can work and deliver a DOS free communication infrastructure. Strength of CAPTCHAs can be enhanced and a lot of work has already been done in this subject. Similarly efficient ACL implementation techniques are also available, which coupled with a thorough behavioral analysis tools can present a DOS free environment, where it will be possible to host critical emergency services as well.

ACLs are used as first line of defense in securing the networks; their proper implementation for a particular purpose is of paramount importance. In order to achieve the best possible results there correct placement is also of paramount importance. Standard fixed ACL has been used in our implementation to show their effectiveness, although it is implemented in a way, to except new connections and their state as well. This architecture will work well in a closely coupled environment. Improvements in ACL handling and increasing the effectiveness of CAPTCHA challenge is desired for fruitful implementation of this architecture.

CONCLUSION AND FUTURE WORK

6.1 Conclusion and Future work

In this work, we have presented a high level architecture to prevent DOS vulnerability of VoIP through use of automated Turing test i.e. CAPTCHA. Albeit high level framework is given and simulated in this thesis, it is intriguing to execute this architecture inside a proper VoIP conventional environment with complete traffic load. The presentation of cryptographic apparatuses is relied upon to present a computational overhead into the CAPTCHA applications, although we can anticipate that this overhead will be mediocre for future computational stages perhaps consolidated with proper execution improvement strategies.

It is possible to increase the effectiveness of ACLs by adding appropriate controls to them. Proprietary hardware like CISCO routers provide rules that are applied to port numbers and IP addresses having list of legitimate hosts permitted to use the service. It is also possible to configure ACLs based on domain names. ACLs can maintain and manage groups also, having inheritances. There is a need to further evaluate the efficiency of ACLs to be implementable on larger and complex network.

Likewise a lot of work is ongoing in the field of text based CAPTCHAs. These are being used for preventing comment spams in blogs, protecting websites registration and for online polls and surveys [31]. We have used a comparatively simple challenge for our simulation; there is a need to test this architecture with more complexes and secure algorithms. The results of the a study to access usability of text based CAPTCHA show that different age groups differ significantly in terms of solving these challenges correctly and also there were differences noted in visual fatigue and workload of different age group [32]. Distortion types have an effect on response time of solving challenge, so with the increase in complexity for bots to solve the challenge, response time of humans to do so also increases. This was the kept in mind while using a simple CAPTCHA challenge for this simulation. Response time also depends on number of characters in an image. There are other types of CAPTCHAs being used such as

anomaly CAPTCHA where six images are presented, five are of same object and sixth is different, that is to be spotted.[33] A research on Image Recognition CAPTCHAs shows that anomaly CAPTCHAs are 90 % correctly solved and with a response time of 42 seconds.

There is a need of further enhancement of ACL effectiveness and CAPTCHA challenge efficiency in future work to be done on the subject. CAPTCHA also serves as a benchmark task for future Artificial Intelligence (AI) technologies. Different other basic AI technologies like fuzzy logic can be used to further strengthen the challenge-response model and also ACL implementation. There is a need to further explore the security options available in this technology. Many implementations of ACL are available; there is a need to test other implementations in VoIP environment.

DOS is becoming the major nightmare in full and expected expansion of VoIP services. Different attacks have been reported in the recent past; yet, the problem at large is an open problem, which needs to be addressed if this technology is to flourish. Disruption of services take a huge toll on finance and customer satisfaction with the services, likewise it is a major hurdle in not implementing this communication technology in banking and other corporate sectors where transactions of money are involved, there is a need to further explore this topic. This research is aimed at opening a new way of countering this vulnerability. This architecture can be further strengthened and improved and is required to be tested in a full grown network environment with full load of traffic.

VoIP is fast becoming the future of communication technology. With the advent of mobile communication, there is a requirement to give more thought on securing and easing VoIP communication in mobile networks. Although different VoIP services like whatsapp, skype and google talk etc. are commercially available but these services have not come up as a substitute of PSTN communication. With the increase in processing powers of mobile devices and increase in the efficiency of IP network, it would be possible. There is a need to address the security issues in depth especially DOS issues, which have a long history in web environment are one of the most potent threat in securing the web applications. There is a potential of misuse of VoIP vulnerabilities to an extent that it can be used by terrorism networks, growing around the world. Terrorist networks can use the vulnerabilities of VoIP to impersonate as a legitimate user and

spread terrorist agenda by messaging or other means in the network, this example is the least that can be done by a terrorist organization. Strong checks on integrity and confidentiality of communication is required. Hence, there is a need to further research this topic and research community should work in this direction as well. World has become a global village and communications is the core of this global village which needs to be secured. VoIP can become the future of communication technologies because of huge internet infrastructure around the world, which can be used to provide cheapest form of communication. In order to achieve such expansion, there is a need to further strengthen the security traits of this technology.

BIBLIOGRAPHY

- [1] “A Survey Paper on Voice over Internet Protocol (VOIP)” by Urjashee Shaw et al. International Journal of Computer Applications (0975 – 8887) Volume 139 – No.2, April 2016. www.ijcaonline.org/research/volume139/number2/shaw-2016-ijca-909112.pdf.
- [2] “An empirical study of security of VoIP system” by Ahmad Ghafarian et al SAI Computing Conference (SAI), 2016. <http://ieeexplore.ieee.org/document/7556105>”.
- [3] RFC-3261. “Session Initiation Protocol”.
- [4] “A Comprehensive Survey of Voice over IP Security Research” by Angelos D. Keromytis, Senior Member, IEEE. Article in IEEE communication survey and Tutorial iv (99): 1-24 Jun 2012.
- [5] “Security Aspects of SIP based VoIP Networks: A Survey” by V.Srihari & P.Kalpna, IEEE Conference Number – 33344 July 8, 2014, Coimbatore, India.
- [6] Point Topic <http://point-topic.com/wp-content/uploads/2013/02/Point-Topic-Global-VoIP-Statistics-Q1-2013.pdf>.
- [7] <https://www.voip-info.org/wiki/view/VoIP+Providers+Pakistan>.
- [8] “Misuse Patterns in VoIP, Security “ J. C. Pelaez, E. B. Fernandez and M. M. Larrondo-Petrie,
- [9] DoS/DDoS Attacks and Protection on VoIP/UC Presented by: Siper Systems. fr.security.westcon.com/documents?documentId=35680...f...Attacks_on_VoIP...
- [10] *Smith, Steve*. "5 Famous Botnets that held the internet hostage". *tqaweekly*. Retrieved November 20, 2014.
- [11] A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment, Michael Glenn August 21, 2003 GSEC Practical Version 1.4b Option 1, © SANS Institute 2003
- [12] <https://developers.facebook.com/docs/facebook-login/reauthentication>
- [13] “Anti-vamming Trust Enforcement in Peer-to-peer VoIP Networks,” by N. Banerjee, S. Saklikar, and S. Saha, in Proceedings of the International Conference on Communications and Mobile Computing (IWCMC), pp. 201–206, July 2006.

- [14] “Detecting SPIT Calls by Checking Human Communication Patterns,” by J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald. In Proceedings of the IEEE International Conference on Communications (ICC), pp. 1979–1984, June 2007.
- [15] “A VoIP anti-Spam System based on Reverse Turing Test,” by T. Wang, Master’s Thesis ETD-05072007-173147, North Carolina State University, May 2007.
- [16] “User-centric, Privacy-Preserving Adaptation for VoIP CAPTCHA Challenges” A. Tasidou¹, P.S. Efraimidis¹, Y. Soupionis², L. Mitrou^{3,2} and V. Katos. Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012) 139
- [17] "Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use" by Bigham, J. P. and Cavender, A. C. (2009), Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA, 2009, pp. 1829-1838.
- [18] "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", Soupionis, by Y. and Gritzalis, D. (2010), Computers & Security, Volume 29, Number 5, pp.603-618, ISSN: 0167-4048.
- [19] “Designing a Secure Text-Based CAPTCHA” by Kiranjot Kaur*, Sunny Behal, Department of Computer Science Engineering S.B.S state technical campus Ferozepur, Punjab, India. 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
- [20] “Emerging Challenges for Security, Privacy and Trust” pp 25-38 “Audio CAPTCHA for SIP-Based VoIP” by Yannis Soupionis, George Tountas, Dimitris Gritzalis. IFIP International Information Security Conference SEC 2009:
- [21] “Security considerations for voice over IP systems” by D Richard Kuhn, Thomas J Walsh, and Steen Fries. NIST special publication, pages 800{58, 2005).
- [22] “Request Header Integrity in SIP and HTTP Digest Using Predictive Nonces,” by J. Rosenberg, expired Internet draft, work in progress, IETF, June 2001. draft-rosenberg-sip-http-pnonce-00.txt.
- [23] www.voip-sip-sdk.com
- [24] <https://www.networkworld.com/article/2181743/voip/massive-ddos-attacks-a-growing-threat-to-voip-services.html>

- [25] “An approach to resisting malformed and flooding attacks on SIP servers” by SuM Y, Tsai CH.. *Journal of Networks*. 2015; 10(2):77–84.
- [26] “SIP proxies: New reflectors in the internet” by Zhang G, Pallares JJ, Rebahi Y, Fischer-Hubner S. *Communications Multimedia Security*; Springer : Verlag Heidelberg; 2010
- [27] <http://www.voipsa.org/Activities/taxonomy.php>
- [28] “Comprehensive comparison of voip sip protocol problems and cisco voip system” by Dr Talal al-kharobi1 and Mohmmmed Abdullallah Al-Department of Computer Engineering, King Fahd University of Petroleum & Minerals(KFUPM), Dhahran, Saudi Arabia *International Journal of Network Security & Its Applications (IJNSA)*, Vol.4, No.4, July 2012
- [29] Stalling W. *Transport-level security. Cryptography and Network Security*, NJ; 2011 p. 485–20
- [30] <https://telegate.com.au/resources/top-5-voip-and-ip-pbx-security-issues/>
- [31] Official CAPTCHA website <http://www.captcha.net/>
- [32] “Usability study of text-based CAPTCHAs” by Ying-Lien Lee ↑, Chih-Hsiang Hsu, Department of Industrial Engineering and Management, Chaoyang University of Technology, Taichung County 413, Taiwan published in Elsevier journal. www.elsevier.com/locate/displa
- [33] “Image Recognition CAPTCHAs” by Monica Chew and J. D. Tygar, UC Berkeley. Cs.berkeley.edu.