Design Implement and Deploy Security Mechanisms for Session Initiation Protocol

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science and Engineering

Submitted By
Sheetal
(Roll No. 801032023)

Under the supervision of:
Dr. Maninder Singh
Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2012

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Design, Implement and Deploy security mechanisms for Session Initiation Protocol"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Maninder Singh and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Sheetal
(Sheetal)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Maninder Singh)
Associate Professor
Computer Science and Engineering Department
Thapar University
Patiala

Countersigned by

(Dr. Maninder Singh)
Associate Professor and Head
Computer Science and Engineering Department
Thapar University
Patiala
27/6

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGMENT

First of all I am thankful to God for blessings and showing me the right decision. With his mercy, it has been possible for me to reach so far.

I would like to express sincerest thanks to my thesis supervisor Dr. Maninder Singh, for his inspiration, guidance, stimulating suggestions, immense help and support throughout the period of this research work. He has provided me with all the necessary resources including motivation and research environment without which it would not have been possible to complete this work. It was a great opportunity for me to do this work under his supervision.

I am thankful to the authors whose work I have consulted and quoted in this work.

I lack words to express my cordial thanks to all my friends for their useful comments and constructive suggestions during all the phases of my life.

Finally, I convey deep sense of gratitude towards my family members for their moral and financial support and encouragement without which it would not have been possible to bring out this thesis

Sheetal

(801032023)

ABSTRACT

Public Switched Telephone Networks (PSTN) is replaced by VoIP now a days and it is widespread in use. VoIP has converged the data and voice into one network. That is called converged network. There are several protocols that support the convergence and VoIP network. These protocols are H.323, Session Initiation Protocol (SIP) and IAX. SIP is a multimedia signaling protocol. It is used to create, modify or terminate sessions with one or more participants involved. This protocol has converged the data, voice, video and messaging into one network. Due to convergence of various networks, it has given rise to various security threats and risks. VoIP networks and SIP is very much vulnerable to the attacks. Due to this, security of SIP is necessary.

In this thesis, VoIP network for SIP protocol is deployed in open source software AsteriskNOW.

Further thesis discusses the various security issues in SIP and implements various mechanisms to defend against different types of attacks. Attacks discussed are Inviteflood attacks and dictionary attacks. Thesis work is implemented and deployed using virtual environment utilizing AsteriskNOW as FreePBX.

Table of Contents

List of Figures

List of Tables

1. INTRODUCTION

1.1 VoIP (Voice over Internet Protocol)

Voice over IP (VoIP), seen as an alternative to the traditional public-switched telephone network is emerging as a successful new trend in telecommunications [1]. It is taking over the traditional PSTN. It is compatible with a variety of platforms (Linux, Windows, mobile devices). It uses a variety of protocols (SIP, RTP, SRTP, SCCP) that depends highly on the data networks and services. VoIP can be a benefit for reducing communication and infrastructure costs. Telephone is definitely an important communication tool. As the Internet is being popular, Voice over IP (VoIP), also called Internet telephony, has become a promising communication medium owing to its economical rates [2]. It offers multiple opportunities such as lower call fees, convergence of voice and data networks, simplification of deployment, and greater integration with multiple applications that offer enhanced multimedia functionality [3]. It is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks [4]. Protocol stack is shown in Figure 1.1.

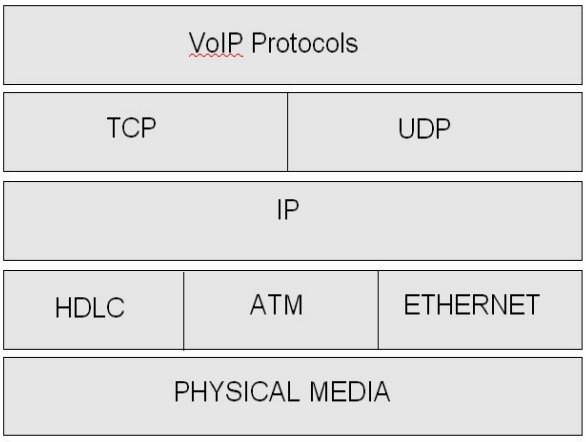


Figure 1.1 Protocol stack [5]

For VoIP environment, some open source softwares are used and that works as PBX too. Detailed description of PBX and softwares is discussed in next sections.

1.2 Private Branch Exchange

Private branch exchange (PBX) is a telephone exchange that connects telephones and other communication devices amongst themselves in a private network. It is basically a switch station to which all telephone lines are connected. It switches the connections by linking the different phone lines. PBX (Private Branch eXchange) is used in many corporations and universities. It centralizes telephone management, consoliates external trunk lines and voice mail [6]. It is a small telephone switch owned by a company or organization. It is owned by different companies to reduce the costs. It reduces the numbers of telephone lines company need to lease form any telephone company. Without a PBX, a company will need to lease one telephone line for every person with a telephone working there. This way it reduces the cost. It is primarily used in business telephone systems to have multi line support for multiple members of staff [7]. It is a business telephone system that will allow any phone in your company to be connected to the same network, be it physically in the office or remotely at a separate location. This type of system will allow you to have specific number dial through to multiple staff members and allow you to transfer calls between any members of staff on the system. The system can be used to simply allow a small firm to have multiple numbers for each department or to have a huge organization communicate internally. It is a privately owned telephone switching system for handling multiple telephone lines without having to pay the phone company to lease each line separately.

PBX Working

PBX is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. PBXs use digital technology. Conversion of digital signal into analog signal is done by plain old telephone systems. The users of the PBX phone system share a number of outside lines for making external phone calls. They can lease only one line and have many people using it with each one having a phone at the desk with different number. The number is not in the same format as a phone number though, as it depends on the internal numbering. Inside a PBX, only need to dial three-digit or four-digit numbers to make a call to another phone in the network. This number is known as extension.

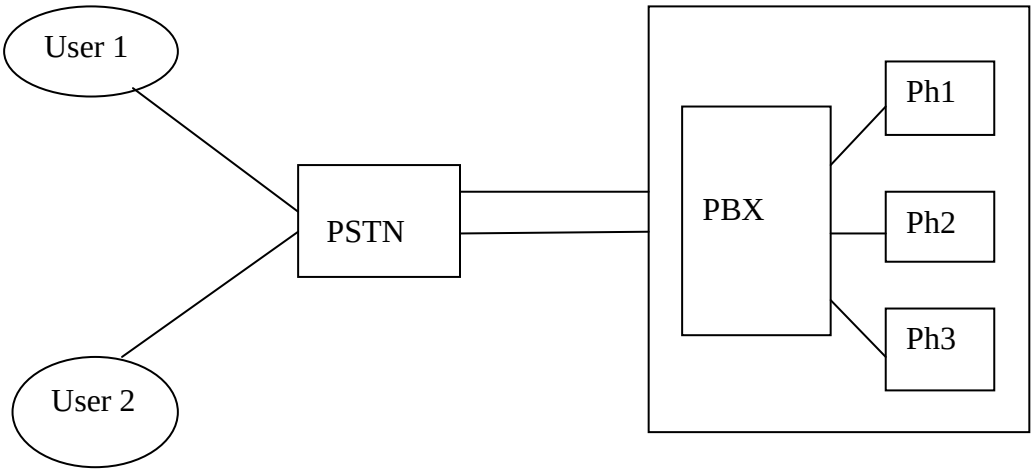


Figure 1.2 PBX working

At starting, PBX was used because it helped in reducing the cost of the enterprise in handling the internal calls. Instead of circuit switching, packet switching was used for communication. As PBXs gained popularity, they started offering various services that were not available initially in the operator network initially such as call redirection, call forwarding, and extension dialing. PBX working is shown in Figure 1.2.

Functions performed by PBX are [6]

- It is used to switch between telephone users thereby creating connections. Only one single number is used by external callers to access all persons in a company or to call a person in company.
- Distribute calls to employees in answering team in an even way; using the Automatic Call Distribution feature.
- User can be offered with menu of options from which he/ she can choose a person to be directed to a particular number using different playback options.
- Allow the use of customized business greetings while answering calls.
- Provide system call management features.
- Place external callers on hold while waiting for a requested person to answer and playing music or customized commercial messages for the caller waiting.
- Record voice messages for any extension from an external caller.

1.3 IP-PBX

A PBX serves a particular business as opposed to a telephone exchange operated by a common carrier or telephone company, connecting outside calls with internal extensions, and internal extensions with each other. Originally PBXs were operated manually, but have become automated over time. Automated PBXs were special purpose computerized devices. A traditional PBX requires separate networks for data and voice transmissions. But this PBX works on technology of converged network that is IP-PBX.

An IP-PBX is a communication server and combination of a switch/router that uses the VoIP protocol. It is able to switch VoIP calls between users on a local network and allows all users to share external phone lines. The server hosts a server-side operating system, such as Linux, Unix or Windows, and an application, such as Asterisk, which delivers the PBX functionality managed through a graphical user interface, such as Free PBX [8].

In an IP PBX, computers can be on a shared LAN that is connected to the IP PBX. Telephones, on the other hand, should be directly connected to the IP PBX. Network telephony embraces both the use of the public switched telephone network (PSTN) and the internet for both voice and data communications. An Internet Protocol Private Branch exchange (IPPBX) is a telephone system designed to operate over a data network in conjunction with the PSTN to deliver both voice and video content. The term “IP” refers to “Internet Protocol.” The term “VoIP” refers to “Voice over Internet Protocol” - the definition relates to the protocol, not necessarily the internet, the protocol can be used on intranets and local area networks, in addition to both private and public wide area networks. Figure 1.3 refers to IP-PBX.

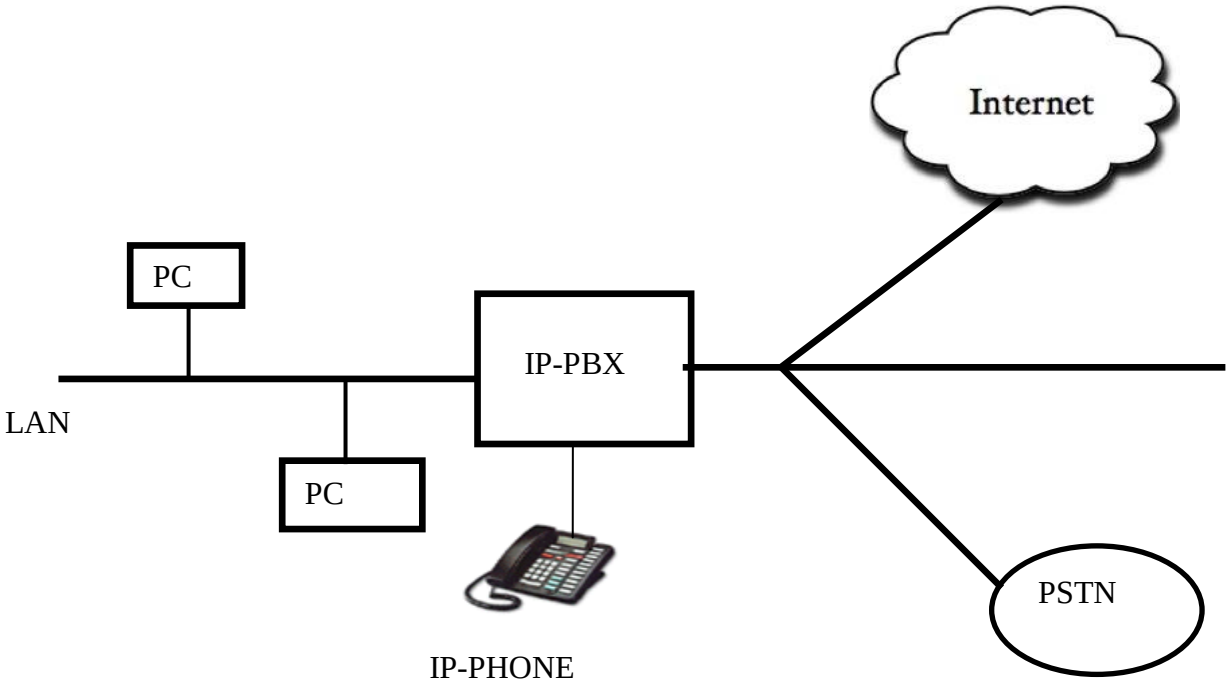


Figure 1.3 IP-PBX

An IP-PBX system combines traditional PBX functionality and voice over internet protocols enabling a business to leverage its intranet to allow users to make internal calls, and external local, long distance, and international calls via the PSTN. IP-PBX systems use either the primary rate interface (PRI) or the session initiation protocol (SIP) for establishing, monitoring, and terminating phone calls. SIP connections usually cost less than those of PRI.

1.3.1 Features

- IP-PBX systems are much easier to install than traditional PBX systems. They are easier to manage by using a web-browser interface that provides current call and systems statuses and historical usages.
- The SIP standard enables the use of non-proprietary IP phones that can be “hot plugged” into any ethernet connection on the intranet, without changing extension numbers. SIP also allows for easy roaming.

- IP-PBX systems have a lower total cost of ownership than both traditional PBX and hosted VoIP solutions because they do not require separate voice and data networks
- IP-PBX systems incur lower long distance costs, and have no incremental costs as more phones are added.
- They offer at least the same functionality as traditional PBX systems, including auto attendant, call queues, call recording, and voicemail.
- IP-PBX systems provide for unified messaging – the ability to receive all messages, including email, fax, and voice in one place.
- They can also provide for integration with applications, such as CRM

An IP PBX also acts as a gateway that provides voice connections (voice lines, T1s) to a LEC, a long distance company, etc. and data connections (cable, DSL, ISDN, E1) to a cable operator, a LEC, an ISP, etc. [9]. IP PBXs can be used bypass the circuit-switched telephone network by using the data network to connect to branch offices and other locations on the data network. Convergence facility was not available in traditional PSTN network. This IP-PBX brought a spark in internet telephony that carries both voice and data together.

An IP PBX replaces a traditional PBX. It can be used with

- an IP phones (with a built-in DSP chip that converts voices to IP packets and vice versa),
- a soft phone (software application on PCs that also converts voice to packets and vice versa), which is used with a headset or a handset,
- existing phones along adapters that packetize voice
- standard phones connected to PCs (PCs acts as the adapters).

IP addresses are assigned to the devices or softphones as they get connected to the system. It means softphones or hardphones can be moved from one location to another. Because extension remains the same as it is defined the configuration files and IP address may get change according to the location.

1.3.2 Advantages of IP-PBX

Compared to a conventional PBX, an IP PBX

- handles both voice and data
- is cheaper since it requires only one network to install and maintain instead of two
- reduces equipment costs
- reduces long distance charges for inter-branch office calls
- is easier to provision
- supports services such as unified messaging,
- is more flexible
- is more scalable
- makes it easier to provide new services, such as data and video collaboration,
- allows remote configuration and supports modular software upgrades, new technologies are easy to incorporate.

1.3.3 IP-PBX Usage

IP PBXs are good for being used particularly in new businesses which will avoid the costs of installing and maintaining two networks. It is easier to maintain one centralized directory than multiple directories and to maintain one single network rather than two different networks.

Some Standards Used in IP PBX Software [9]:

- G.711: An international standard protocol used for encoding (packetizing) telephone voice on a 64 kbps channel.

- G.723: An international standard protocol for compressing voice to 6.4 kbps. The compression quality is very good with voice quality is as good as normal telephone voice quality. It is supported by virtually all IP telephone equipment.

- H.323: Signaling & telephone services protocol for the transmission of IP packets representing any combination of voice, video and data.

- IVR (Interactive Voice Response): A telephone voice system that interacts with callers using with a voice menu.

- SIP (Session Initiation Protocol): A signaling & telephone services protocol similar to but simpler than H.323.

1.3.4 Issues with an IP PBX

Two important issues are QoS and reliability:

- QoS issues (jitter and lost packets) arise when using VoIP on the public network.
- QoS issues (jitter) arise when a telephone and a PC are on a shared LAN – voice and data packets compete for the shared LAN.

1.4 CONVERGENCE

Convergence means the merging of the traditional voice and data networks into one shared infrastructure. Network convergence refers to using packet network to conduct voice (telephony), video and data services, and phasing out the traditional circuit switched PSTN (Public-Switched Telephone Network) gradually.

Convergence can refer to previously separate technologies such as voice (and telephony features), data (and productivity applications) and video that now share resources and interact with each other, synergistically creating new efficiencies. Technological convergence is the tendency for different technological systems to evolve towards performing similar tasks. The industry's adoption of a converged network – that is the concept of the convergence of separate telephone, video and data networks into one IP (Internet Protocol) data network is gaining rapid momentum, with many key players in the market focusing on this new concept in infrastructure design. Network convergence is the efficient coexistence of telephone, video and data communication within a single network. The use of multiple communication modes in a single network offers convenience and flexibility not possible with separate infrastructures. Network convergence is also called media convergence [10].

In response to consumer demand, convergence has been evolving on the Internet ever since its inception. Nowadays, texting, Web surfing, VoIP (voice over IP), streaming media, videoconference applications, online gaming and e-commerce are all extensively engaged in by consumers, businesses, educational institutions and government agencies.

1.4.1 CONVERGENCE STANDARDS AND PROTOCOLS

The convergence of voice and data networks has begun to bring changes in the development and delivery of products and services, if it is a small enterprise, medium or large scale enterprise. Main motive of this is to create a single cable for both data and voice. This helps in better and effective communication. As convergence is developing day by day, there is need to know the standards and protocols that help to communicate and provide solutions. IP is considered as transport protocol for data traffic. It is not considered good for converged networks. Because it becomes the reason for jitter and low video quality. Quality of service is major part of converged networks. Therefore it needs protocols to support it very well. So maintaining QS is a major part of the converged network. Because standards for IP voice transmission have not yet matured, interoperability issues exist at all points in the IP network. Today, mainly proprietary voice compression algorithms are used to packetize voice. This means that only like devices can communicate over an IP network. Standards such as Session Initiation Protocol (SIP) and H.323 are maturing to support convergence and communication server used here is Asterisk, is used as PBX.

1.5 ASTERISK-PBX

In general, asterisk (*) is a wild-card character in many places in computer. This wild-card character helped in designing ip-telephony system. Asterisk PBX was originally written by Mark Spencer of Digium dba Linux Support Services, Inc. As it is open source software, so code has been taken from various open source developers [11].

Asterisk is open source software. It is converged telephony system that works on linux.Open-source means any developer can change according to the requirements. In same way, asterisk is used by many developers to do changes in it. It contains software

part of asterisk, installation part and there are domains of asterisk to work upon. It is defined as a framework which has many modules to set up a phone system. Asterisk is a private branch exchange. A PBX is private switch board, connecting to one or more lines on one side to one or more telephone lines on the other side. It helps in voice over internet protocol. It does voice over internet protocol with help of three or four protocol. It is compatible with many telephone standards [12].

It has many features that a normal PBX should have like call recording, automatic call distribution, call redirecting etc. Asterisk does not need any special hardware for VoIP. It takes help of dummy driver installed on it that is zaptel. Asterisk does not need any special hardware for VoIP. If it needs to have communication with other analog equipment like PSTN, it needs special hardware for that, are given by Digium.

Internally, Asterisk uses slinear as the stream format when it needs to convert from one codec to another. Some codecs in Asterisk are supported only in pass-through mode. These codecs cannot be translated. To verify which codecs are installed in system, the console command:
CLI>core show translation
The following codecs are supported:

- G.711 ulaw (USA) - (64 Kbps).
- G.711 alaw (Europe) - (64 Kbps).
- G.722 (High Definition) – (64 Kbps)
- G.723.1 - Only pass-through mode
- G.726 - (16/24/32/40kbps)
- G.729 - Needs licensing (8Kbps)
- GSM - (12-13 Kbps)
- iLBC - (15 Kbps)
- LPC10 - (2.5 Kbps)
- Speex - (2.15-44.2 Kbps)

In the same way, there are many other CLI commands that are used to check peers, for debugging or to check registered phones on the network. Different commands for asterisk are:

CLI> sip show peers

CLI> sip show registry

CLI>set debug on/off

1.5.1 Protocols for Asterisk

Sending data from one phone to another should be easy provided that the data find a path to the other phone on their own. Unfortunately, it doesn't happen this way, and a signaling protocol is necessary in order to establish connections between phones, discover end devices, and implement telephony signaling. It has recently become extremely common to use SIP as a signaling protocol. IAX is another option becoming popular because it works well with NAT traversal and some bandwidth can be saved in trunk mode. Asterisk supports the following protocols. Some protocols are proprietary and some are public protocols.

- SIP
- H.323
- IAX2
- MGCP
- SCCP (Cisco Skinny)
- Nortel UNISTIM

Proprietary protocols

- Skinny/SCCP

  The Skinny Client Control Protocol (SCCP) is proprietary to Cisco VoIP equipment. It is the default protocol for endpoints on a Cisco Call Manager PBX. Skinny is supported in Asterisk, but Cisco phones are connected to Asterisk, it is generally recommended that obtain SIP images for any phones that support it and connect via SIP instead.

- UNISTIM

  Support for Nortel's proprietary VoIP protocol, UNISTIM, means that Asterisk is the first PBX in history to natively support proprietary IP terminals from the two biggest players in VoIP—Nortel and Cisco. UNISTIM support is totally experimental and does not work well enough to put into production, but the fact that somebody took the trouble to do this demonstrates the power of the Asterisk platform.

Public Protocols

H.323

It was developed to transmit voice, data and fax communications across IP based network while maintaining PSTN connection. It uses RTP to transmit through media. H.323 allows for different configurations of audio, video and data. Possible configurations include audio only, audio & video, audio & data and, audio, data and video. Real-time Transport Protocol (RTP) is used to transport data, typically via UDP and provides a timestamp, sequence number, data type and ability to monitor delivery.

Session Initiation Protocol (SIP)

SIP is a signaling protocol. It is application layer protocol used to establish sessions, maintaining sessions and terminating sessions. It also uses RTP to transmit through media. It provides many features like automatic call distribution, call redirection, IVR and many more.

IAX

The Inter-Asterisk eXchange (IAX) protocol is a protocol created by the programmers who brought us Asterisk. IAX pierces Network Address Translation (NAT) easily. Since IAX is not currently an Internet standard, per se, there is no standards body to work through, allowing more rapid improvement and growth. IAX supports the trunking of calls. This means that multiple calls can be combined through a single stream. Through the trunking capability, a significant amount of bandwidth can be saved by not having the overhead of multiple streams.

Comparison of H.323 & SIP

The Session Initiation Protocol (SIP), an application-level protocol for establishing multimedia communications, has gained momentum. SIP proponents has following as advantages of SIP.

IP-based: IP is the dominant protocol both at the edges and in the core of the Internet. As a result, interoperability with ATM and ISDN is not an issue. H.323 carries a lot of extra baggage to make sure that it is interoperable with the other standards in the series.

- Less complex: SIP is a much smaller and less complicated standard that is based on the architecture of existing popular protocols such as HTTP and FTP. On the other hand, H.323 is large and complicated. As a result, H.323 products and services are more expensive to develop.
- Easy to decode/debug: SIP uses a simple format for commands and messages. These are text strings that are easy to decode, and hence, easy to debug. The entire set of messages is also much smaller than in H.323.
- Client/server architecture: SIP messages are exchanged between a client and a server like HTTP messages. This client–server operation mode allows security and management features to be implemented easily in SIP when compared to H.323 calls.
- Easier firewall/proxy design and configuration: SIP commands can easily be proxied and firewalls can be designed to allow/disallow SIP communications. Getting H.323 through firewalls and proxies is much more complicated.
- Extendible and scalable: Because SIP is based on a client/server distributed architecture it is more scalable than H.323, which often requires peer-to-peer communications. Extending SIP is also easier because of its simpler message format and greater experience with similar protocols such as HTTP.

2. LITERATURE SURVEY

VoIP and SIP were discussed in previous chapter; here detailed description of Session Initiation Protocol and security issues of SIP will be discussed. Till date many researches has been done on SIP and they found many issues in SIP and given many solutions for security of SIP. Here different approaches of attacks and how security can be implied on different approaches to secure the VoIP will be discussed.

2.1 Session Initiation Protocol (SIP)

In IP telephony, main complexity lies in signaling process, often referring to call management and call setup process [13]. There are two or three protocols that are given for signaling. SIP is one of them. The specification for SIP is available in form of several RFCs, the most important one is RFC3261 [14]. This is given by IETF (internet engineering task force) under RFC 3261 (request for comment).

SIP is an application layer protocol. It is a signaling protocol. It is used to create, modify or terminate sessions with one or more participants involved. Here, the session is considered to be a set of senders and receivers that communicate and the states kept in those senders and receivers during the communication. Examples of a session are Internet telephone calls, distribution of multimedia, multimedia conferences, distributed computer game [15]. A session between the elements is established using messages. Different methods are given for different messages to understand. These request methods are INVITE, ACK, OPTIONS and BYE. SIP REGISTER and INVITE messages are the pre-dominant messages used by the SIP protocol [16].

SIP protocol is derived from HTTP and it is much like HTTP. It uses request/response model much like HTTP. It is plain text protocol. It is not used to make communication possible, only SIP is needed. SIP is needed to start the communication. For communication to takes place, it takes the help of SDP and RTP. SDP stands for session description protocol and RTP stands for real time protocol. RTP protocol is standardized

by the IETF and used by ITU-T as well to transport real-time data such as voice and video. RTP can work over UDP OR TCP. UDP provides best effort delivery, it uses UDP for reliable communication, and it does not guarantee packet delivery. These protocols help in communication among media. It is a very flexible protocol that can establish and take down any session. It is considered as a key protocol for network convergence. SIP facilitates building converged IP communication networks that integrate and cooperate with existing telecommunication networks and equipments [17]. The protocol has been designed by keeping in mind scalability, easy implementation and flexibility. SIP involves different network elements for communication to occur. SIP network elements are shown in Figure 2.1.

2.2 SIP Network Elements

- User agent: User agent client is an application that which sends requests and user agent server is an application that receives response.

- Proxy server: A proxy server is a server that receives SIP requests from various user agents and routes them to the appropriate next hop. A typical call traverses at least two proxies before reaching the intended callee.

- Redirect server: Sometimes it is better to offload the processing load on proxy servers by introducing a redirect server. A redirect server directs incoming requests from other clients to contact an alternate set of URIs.

- Registrar server: A server that processes REGISTER requests. The registrar processes REGISTER requests from users and maps their SIP URI to their current location (IP address, username, port, and so on).

- Location server: The location server is used by a redirect server or a proxy server to find the callee's possible location. This function is most often performed by the registrar server.

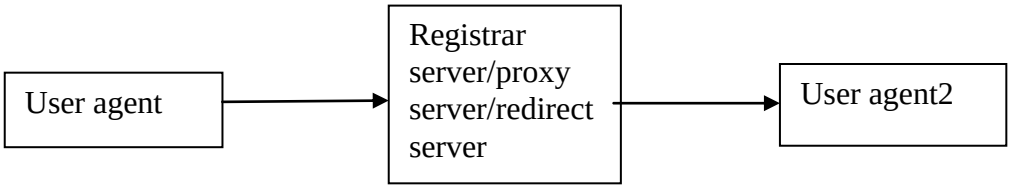


Figure 2.1 SIP Network Elements

2.3 SIP message

SIP is a text based protocol that is based on HTTP protocol [18]. Message syntax and header fields are similar to HTTP/1.1. SIP messages are sent to the clients or devices for communication. They can be classifieds into two groups if they are sent to client or received from server. Message of SIP follow back naur format for message headers. Figure 2.2 refers to SIP Response Message

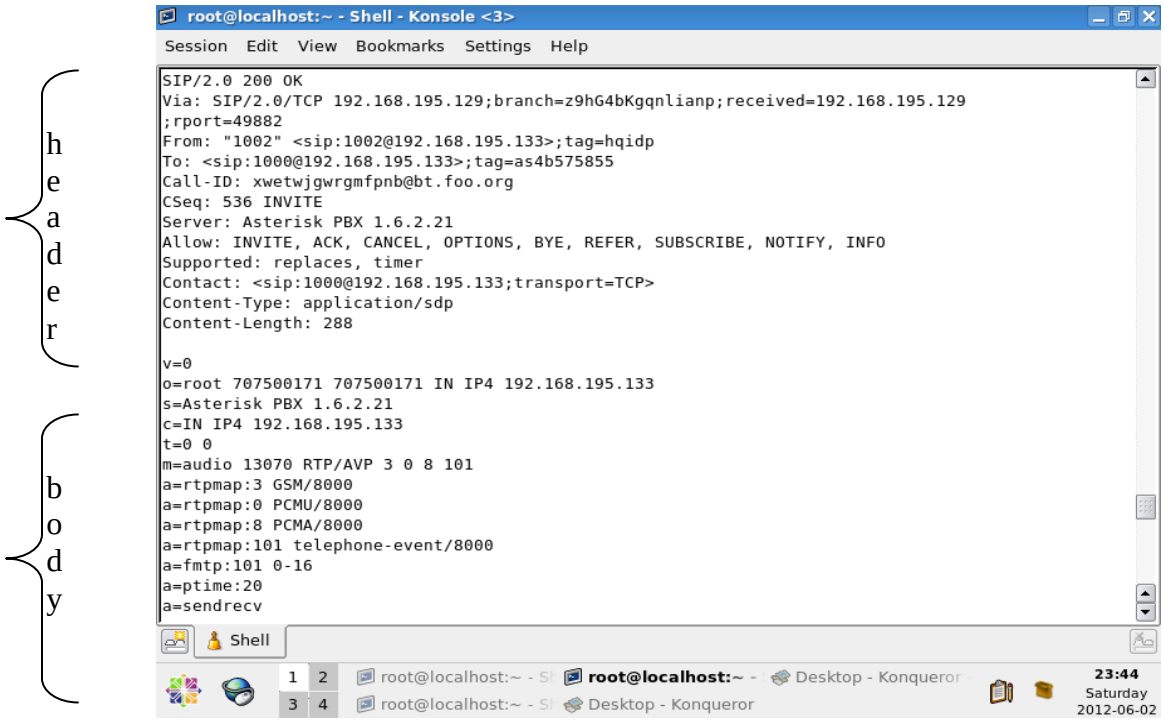


Figure 2.2 SIP Message

2.3.1 SIP Request Methods:

An SIP request is the SIP message sent from a client to a server for the purpose of invoking a particular operation [19]. The method states the primary function of a request that decides what type of the message is and what operations should be executed. SIP uses different request methods [20] that are given in Table 2.1

Table 2.1 SIP Request Methods

INVITE	initiate call
ACK	confirm final response
BYE	terminate (and transfer) call
CANCEL	cancel searches and “ringing”
OPTIONS	features support by other side
REGISTER	register with location service
INFO	mid-call information (ISUP)
COMET	precondition met
PRACK	provisional acknowledgement
SUBSCRIBE	subscribe to event
NOTIFY	notify subscribers
REFER	ask recipient to issue SIP request (call transfer)

2.3.2 SIP Response Messages:

Response codes are 3-digit integer codes that convey the state of the SIP transaction during a response. Response codes range from 1xx to 6xx according to the state and the location from which these responses are being sourced [21]. All SIP Response Messages are described in Table 2.2.

Table 2.2 SIP Response Messages

1xx responses Information responses	**2xx responses Successful responses**
100 Trying 180 Ringing 181 Call Is Being Forwarded 182 Queued 183 Session Progress	200 OK

3xx responses Redirection responses	**4xx responses Request failure responses**
300 Multiple Choices	400 Bad Request
301 Moved Permanently	401 Unauthorized
302 Moved Temporarily	402 Payment Required
303 See Other	403 Forbidden
305 Use Proxy	404 Not Found
380 Alternative Service	405 Method Not Allowed
	406 Not Acceptable
	407 Proxy Authentication Required
	408 Request Timeout
	409 Conflict
	410 Gone
	411 Length Required
	413 Request Entity Too Large
	414 Request URI Too Large
	415 Unsupported Media Type
	420 Bad Extension
	480 Temporarily Not Available
	481 Call Leg/Transaction Does Not Exist
	482 Loop Detected
	483 Too Many Hops
	484 Address Incomplete

	485 Ambiguous 486 Busy Here

5xx responses Server failure responses	**6xx responses Global failure responses**
500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Time-out 505 SIP Version Not Supported	600 Busy Everywhere 603 Decline 604 Does Not Exist Anywhere 606 Not Acceptable

2.4 SIP CALL FLOW

As a beginning of a SIP call, the user client initiates a call by sending an INVITE message towards other user client. That INVITE message is forwarded to the client2 possibly through registrar server or multiple SIP proxies [22]. After that, the client2 receives the INVITE message and replies with a 180 RINGING, which is forwarded towards the client1. At the time when the client2 sends 180 RINGING, it also informs client2 about the incoming SIP call, meaning basically that client's SIP phone rings. If client2 accepts the call that will reply to invitation with a 200 OK message, which includes client2's reply to the SDP received in the INVITE message. This method of offering first a proposition of parameters and in answer receiving accepted parameters is called an offer answer model. When the 200 OK message reaches back to client1 that will indicate client1 the call is answered. SIP call flow is shown in Figure 2.3. Thereafter, SIP client1 sends an ACK message indicating the SIP phone of client2 about the active and accepted session.

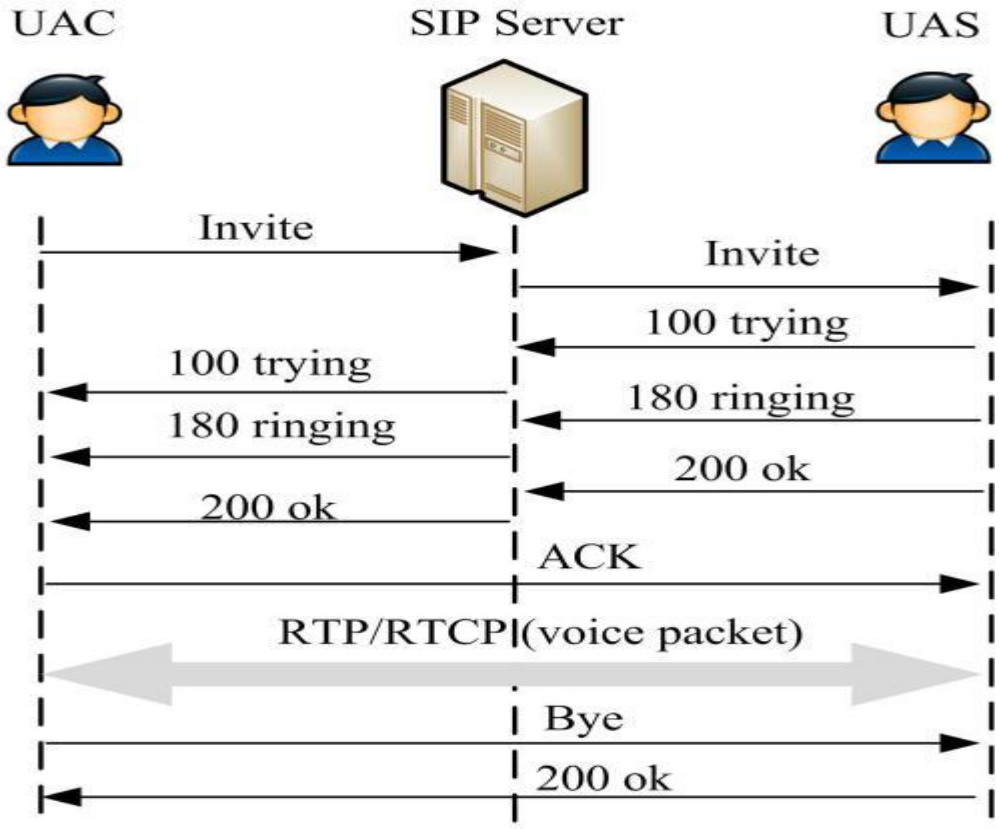


Figure 2.3 SIP Call Flow [23]

From this point on, the client1 sends this ACK message straight to client2, without proxies, and the whole SIP conversation continues peer-to peer. The addresses of the SIP user clients are learnt through header fields in the messages during the exchange of the messages. The ongoing session ends, when either one sends BYE message to the other peer.

2.5 SIP Authentication Mechanism

To receive phone calls, a SIP phone needs to tell a SIP User Agent Server that it is ready to receive the phone calls that are destined to a given extension. This is achieved by sending a REGISTER request to a registrar server [24]. Although not required, REGISTER messages are usually authenticated. The first REGISTER message sent by

the user agent to the registrar does not contain any credentials. As a response, if authentication is required, the registrar then sends back a 401 WWW-Authenticate message, which contains an authentication challenge. The SIP phone computes the challenge response and sends a second REGISTER request which contains the authorization header and the challenge response. If the challenge response is the same as the one expected by the registrar, then the registrar sends a 200 OK response indicating that the user agent has been authenticated. From now on, any calls destined to the registered SIP address will be routed to the authenticated User Agent. For authentication, SIP typically relies on digest authentication, which makes use of MD5 hashing algorithms. Figure 2.4 shows Authentication with SIP Registrar.

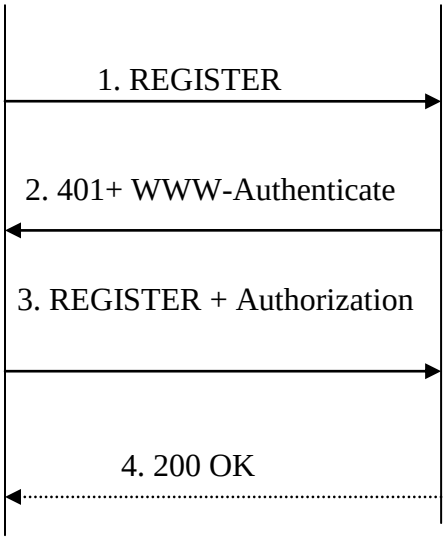


Figure 2.4 Authentication with a SIP Registrar

2.6 AsteriskNOW

AsteriskNOW is an initiative to transform Asterisk in a soft-appliance. The distribution includes CentOS as the operating system and the FreePBX, which is the most used graphical interface [25]. The Zapata project produced an architecture called Zaptel (recently renamed Digium Asterisk Hardware Drivers Interface [DAHDI]). One of the main benefits of this architecture is the ability to use the PC CPU to process media streaming, echo cancellation, and transcoding. In contrast, most existing cards use digital

signal processors (DSP) to perform these tasks. The use of the PC CPU instead of dedicated DSPs reduces the board's price dramatically.

Advantages of Asterisk

- Extreme cost reduction

  Asterisk is very less expensive if it is compared with traditional PBX. It provides all the features like voicemail, IVR, call distribution. Asterisk offers so many features that are not available in low end analog systems.

- Telephony system control and independence

  This is most quoted benefit of asterisk that is the independence. In this manufacturers, gives complete freedom for its configuration. They are not like other manufacturers who do not give passwords or the documentation and they can access their standard interface.

- Easy and rapid development environment

  Asterisk can be extended using script languages like PHP and Perl with AMI and AGI interfaces. Asterisk is open-source, and its source code can be modified by the user. The source code is written mostly in ANSI C programming language.

- Feature rich

  Asterisk has several features that are either not found or optional in traditional PBXs like voicemail, CTI, ACD, IVR, built-in music on hold, and recording. The costs of these features in some platforms exceed the price of the platform itself.

2.7 Overview of an Asterisk system

Asterisk is an open-source PBX that acts like a hybrid PBX, integrating technologies such as TDM and IP telephony. Asterisk is ready to implement functionality such as interactive voice response (IVR) and automatic call distribution (ACD). It is open to the development of new applications.

The main component for an Asterisk Server is the network adapter. A good server network adapter is recommended. CPU is important when there is a need to support high complexity codecs such as g.729 and iLBC and echo cancellation.

2.7.1 Hardware configuration [26]

The Asterisk hardware does not need to be sophisticated. Some necessary steps for hardware configuration.

- Disable unused USB, serial and parallel ports to avoid the consumption of unnecessary interrupts. A robust network interface card is essential.
- Hard disk capacity should be taken care of. PBX used to work in 24*7 mode and desktops cannot afford that capability and it crashes soon. So server machine should be used or system should be designed to work for 24*7 applications.

2.7.2 Software dependencies of asterisk [27]

- LibPRI

  Libpri provides the libraries required for using Primary Rate ISDN (PRI) trunks, as well as a number of other telephony interfaces. Even if there is no PRI line at this time, it can be installed, it does not create any conflicts.

- Dahdi or Zaptel

  Zaptel, containing the Zapata drivers created for Asterisk, is necessary to use Digium's telephony hardware, but also includes a number of libraries that Asterisk depends on, whether we use Digium's hardware or not.

- Asterisk

  Parts of the Asterisk code depend on the libraries included in the libpri package. Therefore, any time libpri is installed, Asterisk should be recompiled.

2.7.3 SIP extensions

SIP is configured in the /etc/asterisk/sip.conf directory and has all the parameters related to SIP phones. SIP clients have to be configured before, to make and receive calls possible.

The section **[general]** includes some parameters to be configured. This is first section to be configured. The main options are:

- allow/disallow: Defines which codecs are going to be used.
- bindaddr: Address to be bound to the Asterisk SIP listener.
- context: Sets the default context for all clients unless it is changed in the client section. Context is defined with different name for security reasons. Unauthenticated users get into this context when the option allowguest is set to yes.
- bindport: SIP UDP port to listen.
- maxexpirey: Maximum time to register (seconds).
- defaultexpirey: Default time to register (seconds).
- register: Registers Asterisk to another host.
- allowguest: Usually set to no to avoid non-authenticated users in the context.

Structure of sip.conf file is shown in Figure 2.5

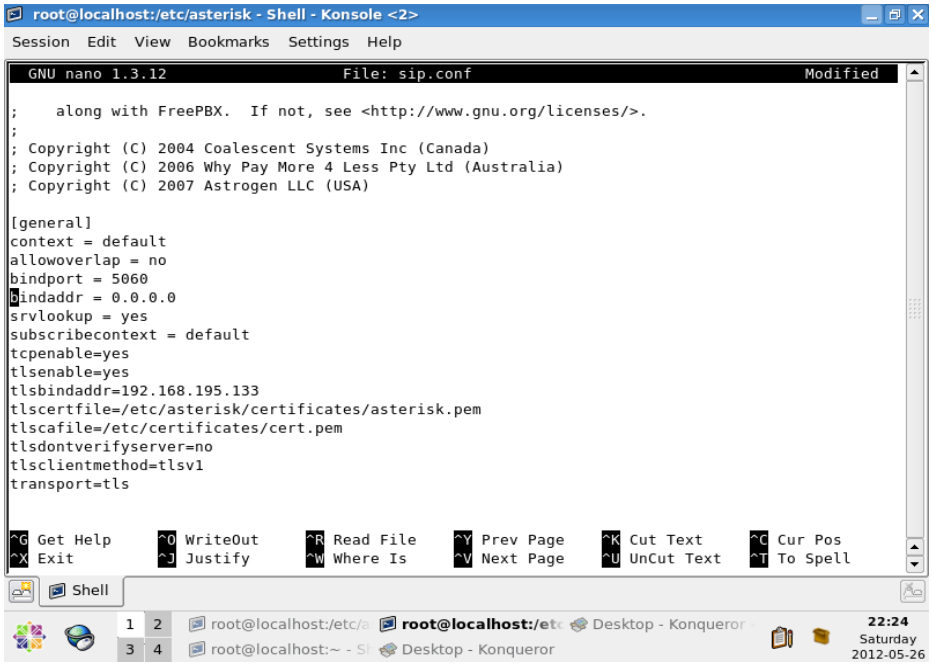


Figure 2.5 Structure of sip.conf file

2.7.4 SIP clients

It is time to set up the SIP clients in /etc/asterisk/sip.conf file after defining all the fields in [general] section.

- name: When a SIP device connects to Asterisk, it uses the username part of the SIP URI to find the peer/user.
- type: Configures the connection class. Options are peer, user, and friend.
  - peer: Asterisk sends calls to a peer.
  - user: Asterisk receives calls from a user.
  - friend: Both occur at the same time.
- host: IP address or host name. The most common option is dynamic, which is used when the host registers to Asterisk.
- secret: Password to authenticate peers and users.

2.7.5 Dial plan introduction

Dial plan is like Asterisk‘s heart. It defines how Asterisk handles every single call to the PBX. It consists of extensions that make an instruction list for Asterisk to follow. Instructions are fired by digits received from the channel or application. In order to configure Asterisk successfully, it is crucial to understand the dial plan. Most of the dial plan is contained in the extensions.conf file in the /etc/asterisk directory. This file uses the simple group grammar and has four major concepts:

- Extensions
- Priorities
- Applications
- Contexts

The structure of the file extensions.conf

The extensions.conf file is separated into sections. The first is the [general] section followed by the [globals] section. The beginning of each section starts with its name definition (i.e., [default]) and finishes when another section is created.

The section **[general]**

To configure the dial plan, it is helpful to know the general options that control certain dial plan behaviors. These options are:

static and write protect: If static = yes and writeprotect = yes, then CLI command can be used to save dialplan. Structure of extensions.conf is shown in Figure 2.6

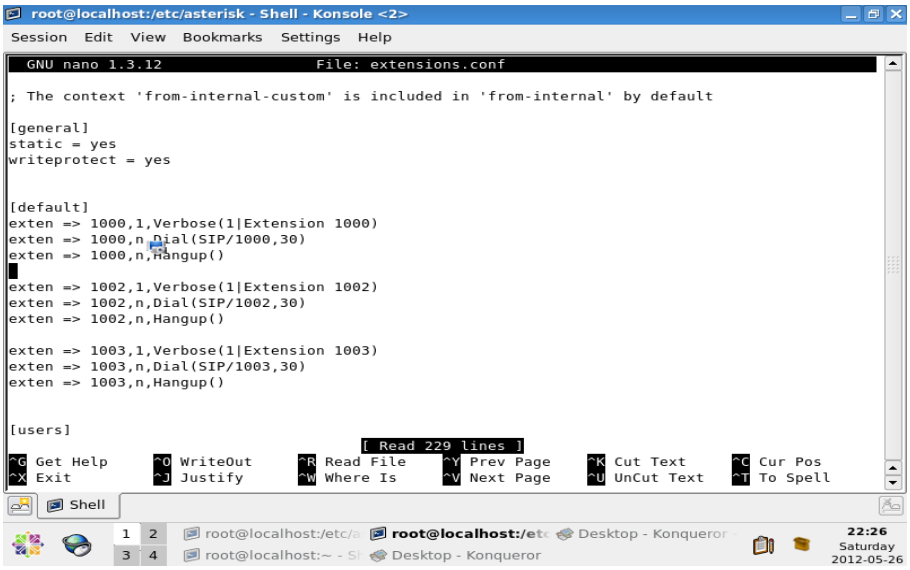


Figure 2.6 Structure of extensions.conf file

2.7.6 Channel configuration files work with the dialplan

Channel configuration (sip.conf) and dial plan files are (extensions.conf). When any number is dialed, then corresponding sip.conf and extensions.conf files are matched. It is shown by Figure 2.7

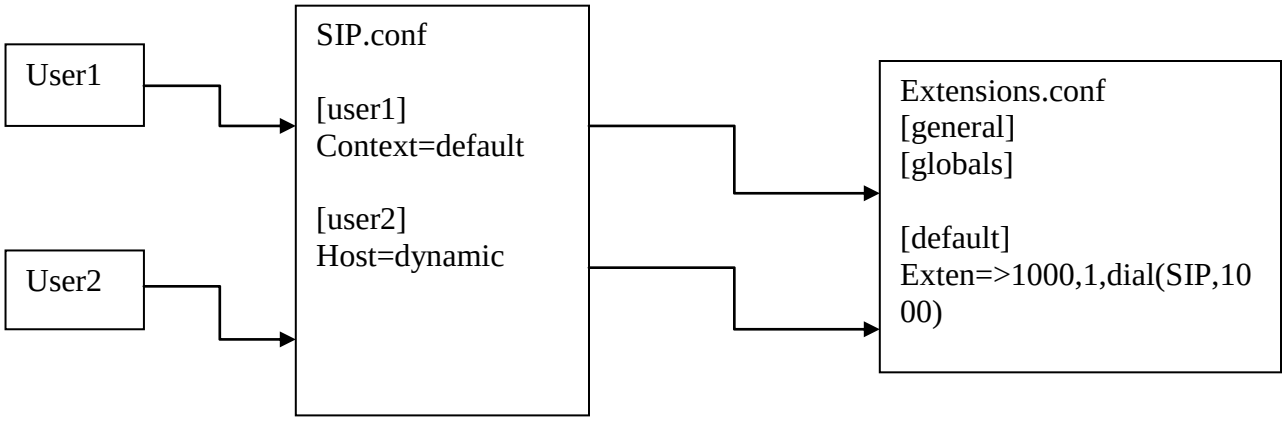


Figure 2.7 Relation of configurations file with dialplan [28]

When a call comes into asterisk, the identity of incoming call is matched, in channel configuration file for the protocol in use. The channel configuration file handle authentication and defines what channel will enter the dial plan. Once asterisk has determined how to handle the channel, it will pass all control to the correct context in dialplan, the context parameter in the channel. Configuration file tells the channel where it will enter the dialplan which contains all the information how to handle and route the call.

2.8 Security

A system is secure when it can protect/deliver the data/services requested, stored or passed within it. The CIA triad (confidentiality, integrity and availability) are the three main widely accepted variables in information security.

Confidentiality

Nowadays, there is a lot of sensitive data being sent over the Internet. Like in VoIP, passwords or files are being sent over the internet and this is considered as very sensitive data. The challenge of protecting this data is increasing as more and more attackers try to steal it by exploiting through vulnerabilities that exist in applications or networks. Security experts define confidentiality as the concept of protecting sensitive data from being viewable or modifiable by an unauthorized entity [29]. Confidentiality can also be regarded as a concept that keeps the information secret from any unauthorized party what is being sent over the network. If data can be sniffed, viewed, or modified by unauthorized parties, then the system in which the data is stored in or transmitted over does not have confidentiality and thus categorized as not secure.

Integrity

Integrity means completeness and accuracy of data. It ensures that received data is not changed by adversary during transmission. Computer networks create a virtual connection between one person and another. Using the Internet, people no longer to be physically present in order to talk to each other because of services like instant messaging or VoIP calling. However, the Internet is a public network. People have to be sure that

the data that they are sending and receiving over the Internet will not be tampered by others. Likewise in SIP, no phones calls should be intercepted by the third person.

Availability

Availability ensures that services and information can be accessed at the time they are required. In other words, the data or services requested by authorized clients have to be available. Sometimes, a service may not be available when users need it. For example, placing or receiving a call in VoIP is one service offered by the VoIP server to legitimate clients. When the VoIP server crashes, consequently the service is no longer available and placing or receiving a call becomes an impossible task.

2.8.1 SECURITY OF SIP

As SIP-based VoIP services are expected to slowly replace the traditional PSTN services, SIP servers are becoming potential targets of various attacks. Thus far, it is safe to claim that VoIP is just another Internet service. Therefore, VoIP systems are exposed to many of the same attacks that predate other Internet services for instance, operating systems vulnerabilities, denial of service attacks, spoofing, and so on. In any case, this section discusses some of the most common threats that prey on VoIP systems.

There are a lot of vulnerabilities in SIP which becomes the reason of exploit. In the same way, it is not secure at the side of authentication too. Many attacks can be done on authentication too. There are many methods or countermeasures are taken to secure SIP authentication and all the countermeasures will be discussed for flooding attacks and authentication attacks i.e. dictionary attack. Security threats of SIP are:

Security threats of SIP are:

Integrity Threats

- Registration Hijacking: This is similar to a man-in-the-middle attacks where an attacker sniffs a REGISTER message from a legitimate user and modifies it with its own address at the contact address [30]. The SIP server will receive this fake message and update the contact address belonging to the legitimate address with

the fake address. All incoming calls for the legitimate contact will be redirected to the fake address.

- IP Spoofing/Call Fraud: This attack is executed by impersonating a legitimate user with a spoofed ID and sending an INVITE or REGISTER message [31]. This attack is easy to do when SIP messages are sent in clear-text. An illegitimate REGISTER message from an attack can cause calls for the legitimate user to be redirected to a random IP address with no user at the other end. An attacker can use a legitimate IP address to make free calls. Call fraud attacks are intended to facilitate the illegal use of the VoIP infrastructure to place free phone calls.

- Weak Digest Authentication: The SIP protocol recommends using the MD5 digest algorithm for authentication. However, this particular hash algorithm is considered too weak for use in systems requiring high security. Additionally, the SIP hash authentication algorithm has minimal header fields which can be forged.

Availablity Threats

- INVITE flooding: This is similar to a SYN flood attack in TCP connections where an attacker can execute a denial-of-service attack by flooding a SIP server with fake INVITE messages.

- BYE Denial-of-Service: When a SIP signaling packet is sent in clear text, it can be tampered with. For example, an attacker sniffing legitimate INVITE messages can forge a legitimate BYE message and send it to one of the UAs in a session and effectively tear-down the session prematurely.

- RTP Flooding: This attack is related to media transmission since most of these transmissions are based on RTP once the session has been created with SIP. An attacker forges RTP packets and bombards either UA in the session which results in degrading the quality of the session or a terminal reboot.

- SPIT (Spam over Internet Telephony): This attack sends unsolicited calls to legitimate users without their consent. At best, such an attack is an annoyance. At worst, it can flood the voicemail system, resulting in a form of denial-of-service.

Confidentiality Threats

- Eavesdropping

  Eavesdropping is the interception, listening, and/or recording of private conversations between parties [5]. Unfortunately, RTP does not include any mechanism to prevent eavesdropping (such as encryption), which allows an attacker listening the network. For instance, with a packet sniffer, to intercept, listen, and record VoIP communications. Eavesdropping attack are a consequence of failing to use appropriate encryption.

- Man in the Middle attacks

  A man-in-the-middle attack occurs when a third party (the attacker) poses as the other party in a communication which allows an attacker to monitor, record, obstruct, or modify passing information. Man-in-the-middle attacks may be as simple as using a packet sniffer to collect, analyze, and alter protocol payloads. Also, it can be as complex as using ARP spoofing to overcome broadcast segmentation in Ethernet networks and therefore to force all IP packets from the calling parties to pass through the attacker's host first [32]. Man-in-the-middle attacks are a consequence of a lack of strong encryption and appropriate authentication in raw SIP-based communication.

- Call hijack

  A call hijack occurs when an attacker effectively controls one end of a VoIP call. Call hijack usually occurs after the call has been set up. The most common type of call hijack attack occurs when the attacker first disable the legitimate party (for instance, using a DOS attack) and then proceeds to alter the registered information about this party in the VoIP Registrar's database [33]. As explained above, SIP-based VoIP communication starts when callers register their

information with the corresponding VoIP Registrar. If an attacker is able to modify this information—for instance, replacing the original IP address with its own address—then the VoIP Proxy will direct all incoming calls to the attacker's IP address instead of the original caller's IP address. As previously mentioned, man-in-the-middle and call hijack attacks are possible because SIP is a text-based protocol that does not implement any type of encryption—SIP messages travel in the clear. SIP also lacks authentication and appropriate integrity check of signaling data.

2.9 FLOODING ATTACKS IN SIP

- SIP Registration Flooding Attack: A user agent send REGISTER request to SIP server when they initially want to communicate with other user and at regular interval [34]. An attacker can easily spoof large number of location addresses and send request to REGISTRAR with invalid username and passwords. In response attacker receives the 401 UNAUTHORIZE messages and again send the invalid MD5 digest calculated by hash function with nonce, realm, username and password values When SIP server receive the calculated MD5 digest it will match the received digest to digest calculated by server, while doing so server lookup the database of users and engaged in calculating digests. Due to excessive calculation of unwanted MD5 digest and to lookup user directory server incur high load on server and cross the threshold value of packet processing and hence cause the DoS attack.

- Authentication Flooding Attack: The authentication mechanism used by SIP is based on HTTP Digest mechanism based on challenge/response model. In order to verify the valid password sent by client, SIP server needs to compute MD5 Digest response to match the received response. The attacker machine needs not to calculate the MD5 Digest response using the realm, nonce, username and passwords values. An attacker can easily send the random Digest values stored. Using this mechanism an attacker can send more requests per second to target server to keep server busy.

- INVITE Flooding Attack: The SIP infrastructure is also vulnerable to INVITE flooding attack. A VoIP server should have a security feature to blocks flooded call request from unregistered clients. So, an attacker registers first after spoofing a legitimate user, and then sends flooded INVITE requests in a short period of time with different rates. This impacts significantly the performance of SIP server.

- PING Flooding Attack: VoIP protocol uses ping message in the application layer to check out the reachability of server, like SIP OPTIONs message. A router or firewall do not allow (Internet Control Message Protocol) ICMP ping in many production network for security reason. However a VoIP system should allow ping message in application layer for more reliable service ability, but an attacker can misuse this message and can flood the SIP server with various ping messages. Beside of these major flooding attacks, an attacker can flood valid or invalid call control messages like SIP INFO, NOTIFY, Re-INVITE etc. after call set up.

3. PROBLEM STATEMENT

The open architecture of the Internet and the use of open standards like Session Initiation Protocol (SIP) constitute the provisioning of services vulnerable to known Internet attacks, while at the same time introducing new security problems based on these standards that cannot been tackled with current security mechanisms. This describes security problems in the SIP protocol that may lead to denial of service. Such security problems include flooding attacks, security vulnerabilities in parser implementations and attacks exploiting vulnerabilities at the signaling-application level.

Objectives

1. To study and explore the various security issues in Session Initiation Protocol.
2. To design and implement layer 7 firewall system to secure the Session Initiation protocol.
3. To deploy and test secure IP PBX in virtual environment.

4. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Experiment was performed using some softwares. These softwares are:

1. AsteriskNOW
2. Softphones

4.1 AsteriskNOW

AsteriskNOW is a framework for asterisk users. It is free PBX software provided by digium. Digium also produces telephony interface cards and other hardware for Asterisk's PBX. It provides a user friendly interface with different choices. Asterisknow is built for those who want to establish telephony applications or custom solutions with asterisk. AsteriskNOW is an initiative to transform Asterisk in a soft-appliance. The distribution includes CentOS as the operating system and the FreePBX, which is the most used graphical interface. FreePBX is shown in Figure 4.1.

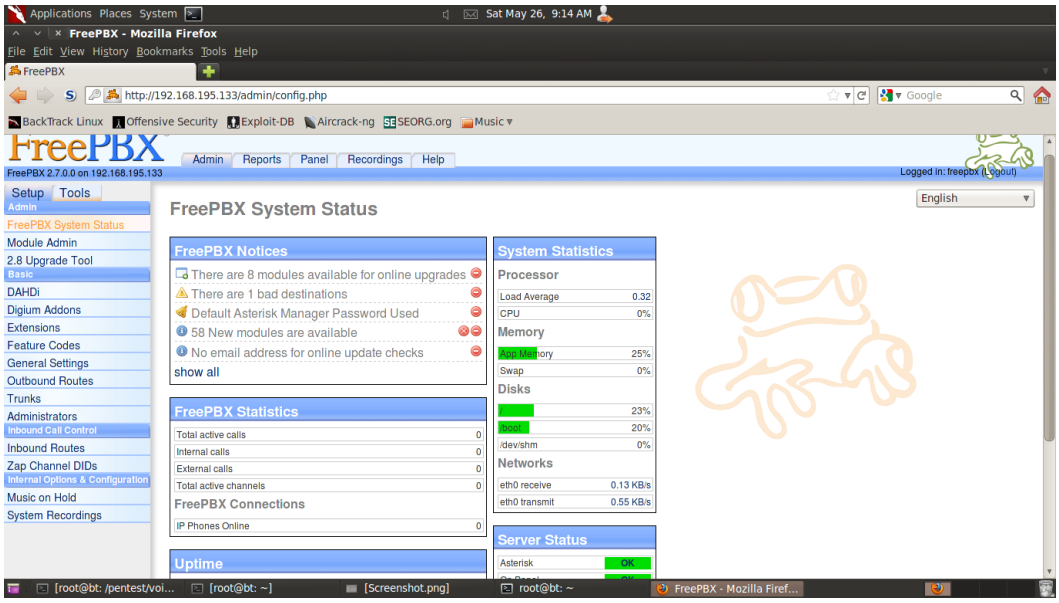


Figure 4.1 FreePBX

4.2 Softphones

A softphone is software that runs on laptops or desktops. Softphones uses the sound system of laptops for communication. It needs headsets to call through. Now days these applications are also used for cellular phones for same and different networks. These phones are portable and economical than hardphones. Softphones used over here are:

4.2.1 X-LITE [35]

This phone is given by Counterpath Corporation. It is a SIP based softphone which works with many networks. It has choice of dial pad-centric or contact centric interface or a combination. X-LITE softphone is shown below in Figure 4.2.

Figure 4.2 X-LITE softphone

4.2.2 Minimum requirements

Minimum requirements of hardware and software for X-LITE defined by Counterpath Corporation are shown in Table 4.1.

Table 4.1 Minimum requirements for X-LITE

Processor	Pentium 4® 2.4 GHz or equivalent
Memory	1 GB RAM
Hard Disk	50 MB
Operating system	Microsoft Windows XP Service Pack 2 Microsoft Windows Vista, 32-bits and 64-bits arch Microsoft Windows 7 Mac OS 10.5 or above
Connection	IP network connection (broadband, LAN, wireless); Constant Internet connection
Sound adapter	Full-duplex, 16-bit or USB Headset

4.2.3 Twinkle [36]

Twinkle is available for Linux only. It is softphone for VoIP and works on session initiation protocol. This phone is used for phone to phone communication and for same or different networks using SIP proxy. It is open source phone and it follows the open standards SIP/SDP/STP. Twinkle softphone is shown in Figure 4.3

Features

- Its integration with kde address book.
- Call history
- Voice calls
- Ring tones
- Dtmf

- multiple identities.

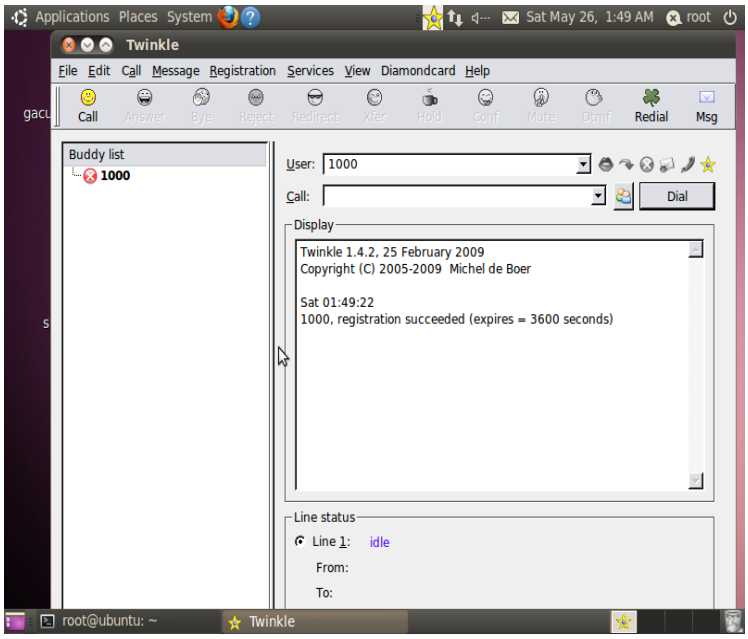
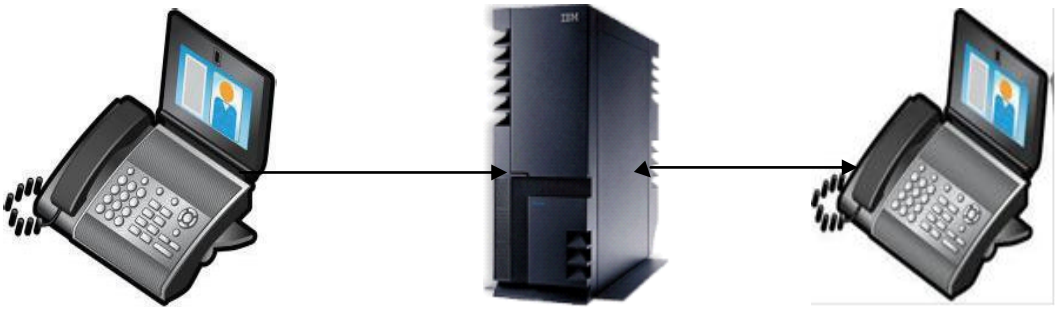


Figure 4.3 Twinkle softphone

4.3 Experiment setup

Asterisknow here acts as freepbx. Asterisk acts as registrar server and redirect server. Two phones have been taken, one is twinkle on linux distribution and x-lite on other windows machine. Experiment setup is shown in Figure 4.4.



User 1 Registrar server User 2

Figure 4.4 Experiment Setup

One phone sends INVITE request to another phone with the help of registrar server that can act as a proxy server too. Registrar server helps in registration of both of the phones, and sends REGISTER message as both phones needs to be registered. It matches the data from SIP.conf file for registration and authentication and corresponding to it, extensions.conf plays its role. Registration of softphones on registrar server is shown in Figure 4.5. It is captured using wireshark (sniffer) on vmware workstation.

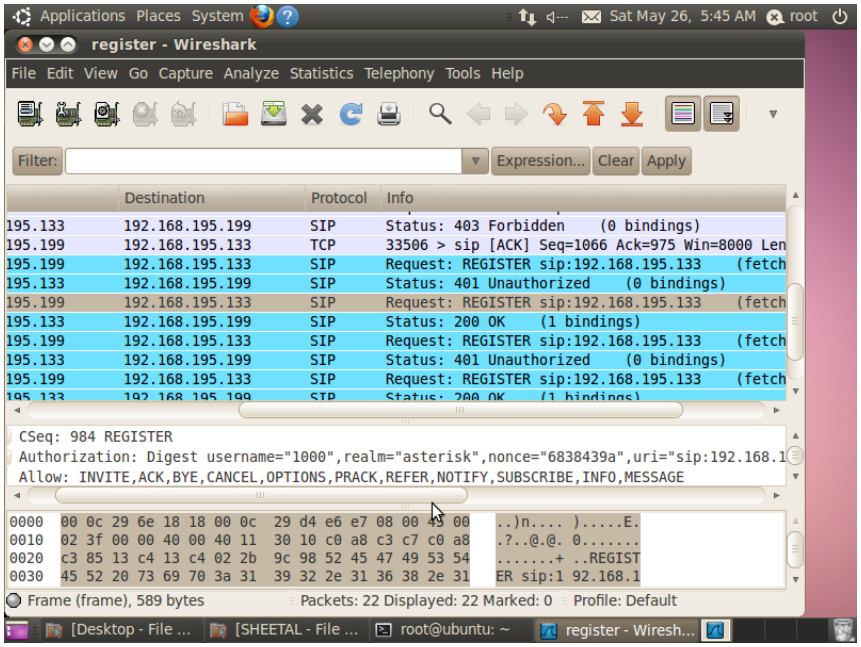


Figure 4.5 Registration of softphones

Then call establishment starts with TRYING and RINGING SIP messages. Call is established and data is sent by real transport protocol (RTP) using codecs. When user hangs up the call, he sends bye message to the other user through registrar server and ack is sent by another user as a reply and with 200 OK message, call is terminated. Graph analysis Of BYE message is shown in Figure 4.6

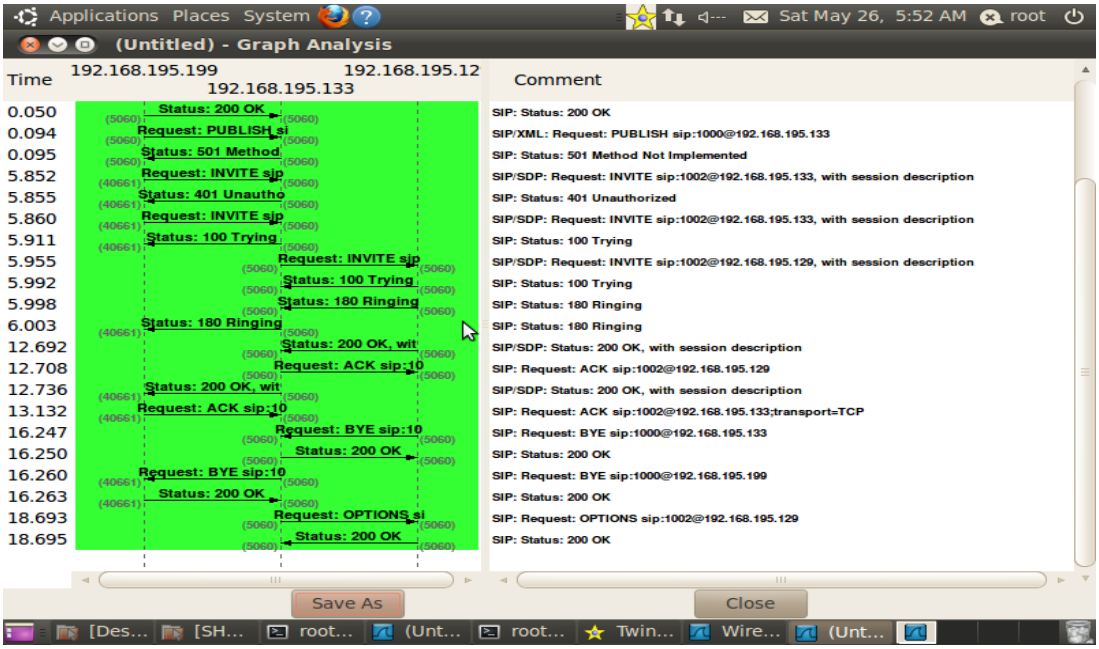


Figure 4.6 Graph showing BYE message

It is all about the phones, registration, call establishment and call termination. Due to some vulnerabilities, this setup can be hacked.

4.4 Hacking of SIP network

To hack the SIP network setup, first thing need to do is information gathering. SIP devices present in the network are discovered by scanning, enumerating and fingerprinting. After discovering the devices present on the network, different types of attacks can be done like UDP flooding, INVITE messages flooding, traffic interception, eavesdropping, session teardown, specific attacks with REGISTER messages, RTP media injection/ mixing. There are various tools for information gathering, fingerprinting and enumeration. In VoIP environment, information required for network is PBX IPaddress, softphones IP addresses and extensions. Information gathering can be done by using **SMAP**. It is a simple scanner for SIP enabled devices.

In the same way, there is one more scanner svmap. It is a simple scanner for SIP enabled hosts. It can scan single host or entire subnet. It is shown in Figure 4.7

Figure 4.7 scanning of network using **svmap**

This gives us the IP addresses of SIP enabled devices present on the network and information related to it.

During VoIP enumeration, extension enumeration is also important to identify the live SIP extensions. **Svwar** aides in scanning complete range of IP addresses. It also tells, is there any need of authentication or not. It is shown in Figure 4.8

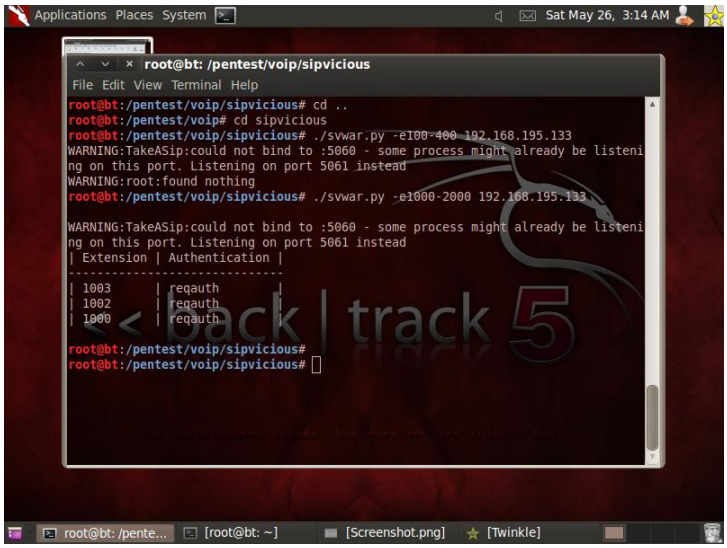


Figure 4.8 Extensions enumeration

It has given the extensions present over the network and some information of authentication. Here, it is **reqauth.** It means authentication is required for these extensions. Now, information regarding ip addresses and extensions has been gathered needed for different type of attacks.

4.5 Inviteflood attack on asterisk

To do inviteflood attack, there is a need of ip address of server and valid extensions. Valid extensions and ip address has been enumerated using various tools like smap, svmap and svwar. For inviteflood attack, inviteflood tool is used that is a great traffic generator. It sends many INVITE request messages simultaneously. It hangs up the PBX server and user devices both. Server cannot handle so many invite requests at a time and goes into busy state. Here, for inviteflood attack, devices used are:

- Twinkle softphone (Victim)
- X-lite softphone (Victim)
- AsteriskNOW (PBX)
- Backtrack5 R1 (Attacker)

On asterisk, wrong extensions with valid IP address of asterisk are tested and it gives some different errors in different scenario. It is shown in Figure 4.9 and 4.10. Command to do inviteflood attack on backtrack machine as a root user is

 # ./inviteflood eth0 200 192.168.195.133 192.168.195.133 100000000

Figure 4.9 Inviteflood on asterisk

At the time of inviteflood, packets are also captured using wireshark which is shown in Figure 4.10

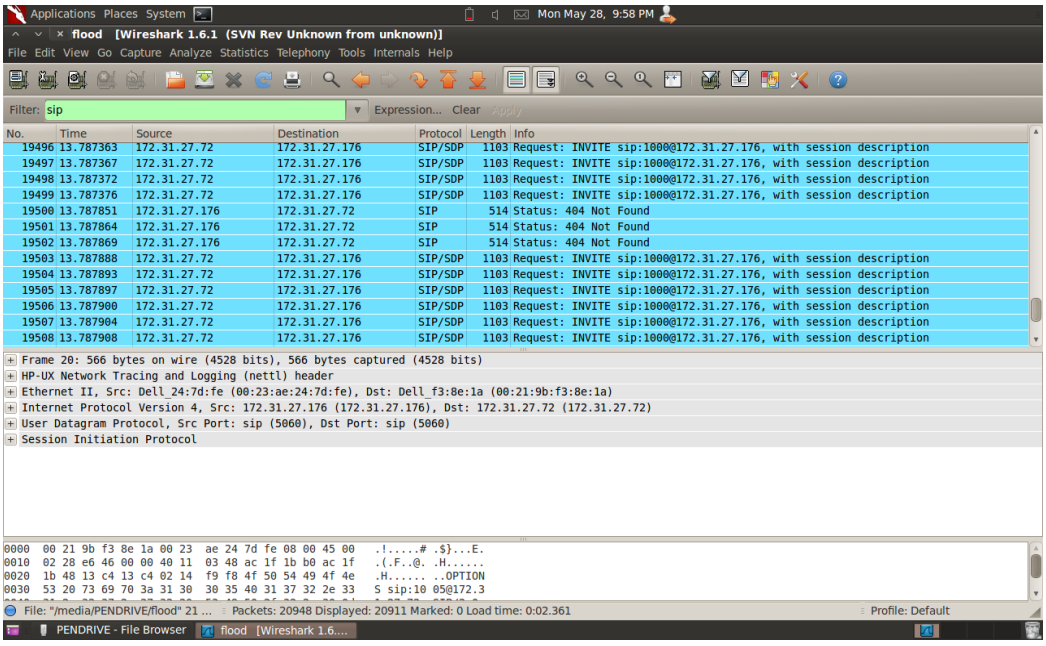


Figure 4.10 Wireshark capture of inviteflood

As it keeps on sending INVITE requests, there must be something to prevent the inviteflood on asterisk and softphones. To stop invite flooding attacks stateful firewalls

are used. It is type of firewall that attempts to track the state of network connections when filtering packets. The stateful firewall's capabilities are somewhat of a cross between the functions of a packet filter and the additional application-level protocol intelligence of a proxy. Stateful firewalls used here are IPTables. Sometimes SIP Servers are attacked by hacker with huge number of SIP registration and a lot of invite requests which make SIP Server mad. Due to which server may halt and SIP phones stop working and go into busy state for some period of time. To overcome this problem, it can be blocked easily by IPTables.

4.6 Layer 7 Firewall

IPTables is used to set up, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table. Connection tracking records the state of a connection based mostly on protocol specific information. Administrators create rules specifying what protocols or specific traffic types should be tracked [37]. When a connection is begun using a tracked protocol, IPTables adds a state table entry for the connection in question. This state table entry includes such information as the following:

- The protocol being used for the connection
- The source and destination IP addresses
- The source and destination ports
- A listing with source and destination IP addresses and ports reversed (to represent response traffic)
- The time remaining before the rule is removed
- The TCP state of the connection (for TCP only)

To check the default IPTables rules command used is.

 # iptables –L

It is shown in Figure 4.11

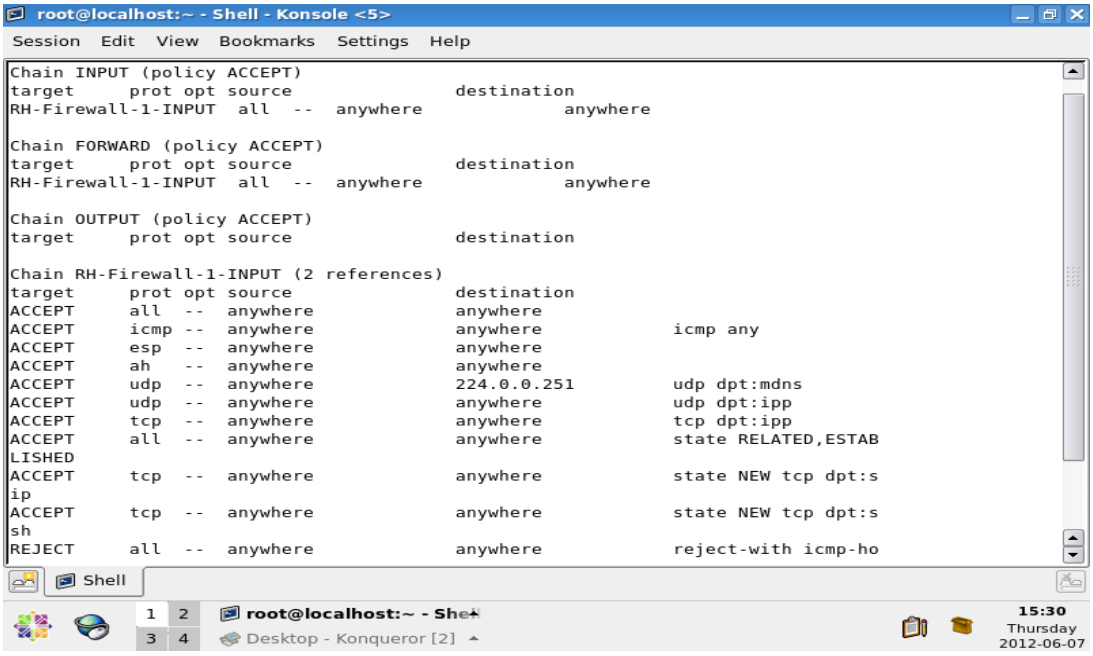


Figure 4.11 IPTables listing

Sometimes, the default IPTables rules create problem in registration of SIP phones. This problem comes due to rejection of ICMP-HOST. Because it does not allow ICMP packet to go inside the network. Deleting that rule helps in registration of phones.

These are some very basic access rules of IPTables.

 # iptables -P INPUT ACCEPT

This sets the default policy on the input chain to ACCEPT.

 # iptables –F

This is the command to flush the current rule set and only use the defaults.

 # iptables -A INPUT -i lo -j ACCEPT

This is a simple rule to allow all access from the loopback adapter. The -A switch means to append a new rule to the chain. -i means this rule has to do with all traffic flowing through a network interface (in this case, the lo or loopback interface). -j means to Jump to the ACCEPT action.

 # iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

-m switch, is used to load a module. Here module is 'state'. The state module is able to examine the state of a packet and determine if it is NEW, ESTABLISHED or RELATED. NEW refers to incoming packets that are new incoming connections that weren't initiated by the host system. ESTABLISHED and RELATED refers to incoming packets that are part of an already established connection or related to an already established connection.

 # iptables -P INPUT DROP

This line changes the default policy for the INPUT chain back to DROP, which is what is required to actually block traffic coming into your server.

 # iptables -P FORWARD DROP

This rule is also used to DROP the packets sama as INPUT chain except that default policy for the FORWARD chain, which handles traffic flowing through our system from one interface to another.

 # iptables -P OUTPUT ACCEPT

And finally, this rule allows all traffic to flow outwards from server.

To apply the same chain rules next time at the time. It should be saved. Commands to save iptables are:

 # iptables-save

or

 # service iptables save

IPTables rules specific to asterisk

To run asterisk on server that got protected with IPTables, some few specific rules are setup. These rules are:

 # iptables -A INPUT -p udp -m udp --dport 5060 -j ACCEPT

This rule is used when data is coming from UDP port for SIP traffic.

iptables -A INPUT -p udp -m udp -s 172.19.240.24 --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m udp -s 172.36.15.0/24 --dport 5060 -j ACCEPT

 # iptables -A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT

This is the rule that allows RTP traffic. By default, asterisk uses a large range of rtp ports to establish rtp connections

iptables -A INPUT -p udp -m udp --dport 10000:10050 -j ACCEPT

 # iptables -A INPUT -p udp -m udp --dport 4569 -j ACCEPT

This rule is for IAX2 connections. IAX2 is another VoIP protocol, much like SIP. Unlike SIP, it only needs one port open on your firewall for both control traffic and audio / data traffic.

 # iptables -A INPUT -p tcp -m tcp --dport 5038 -j ACCEPT

This rule is to allow connections to the Asterisk Manager Interface, or AMI.

These are some basic rules that need to be applied when asterisk server firewall is used. But to protect the asterisk from the inviteflood attack, some specific rules are used and these are shown in Figure 4.12

Iptable rules to stop inviteflood attack are:

Iptables –A INPUT –m iprange –src-range 192.168.195.1-192.168.195.254 –p tcp –i eth0 –sport 5060:5061 –j ACCEPT.

Iptables –A INPUT –m state –state NEW, ESTABLISHED,RELATED –p tcp –dport 5060:5061 –m limit –limit 6/s –j ACCEPT.

Iptables –I INPUT –p udp –m string –string “INVITE” –algo bm –m hashlimit –hashlimit 6/s –hashlimit –mode scrip, dstport –hashlimit-name tunnel_limit –m udp –sport 5060 –j ACCEPT.

Iptables –I INPUT –p udp –m string –string “REGISTER” –algo bm –m hashlimit –hashlimit 6/s –hashlimit –mode scrip, dstport –hashlimit-name tunnel_limit –m udp –sport 5060 –j ACCEPT.

Iptables –A INPUT –m state –state NEW –p udp –i eth0 –dport 5071:65535 –j queue

Iptables –A INPUT –m state –state NEW –p udp –i eth0 –dport 1024:5059 –j queue

Iptables –A INPUT –m state –state NEW –p udp –i eth0 –dport 5060:5070 –j queue

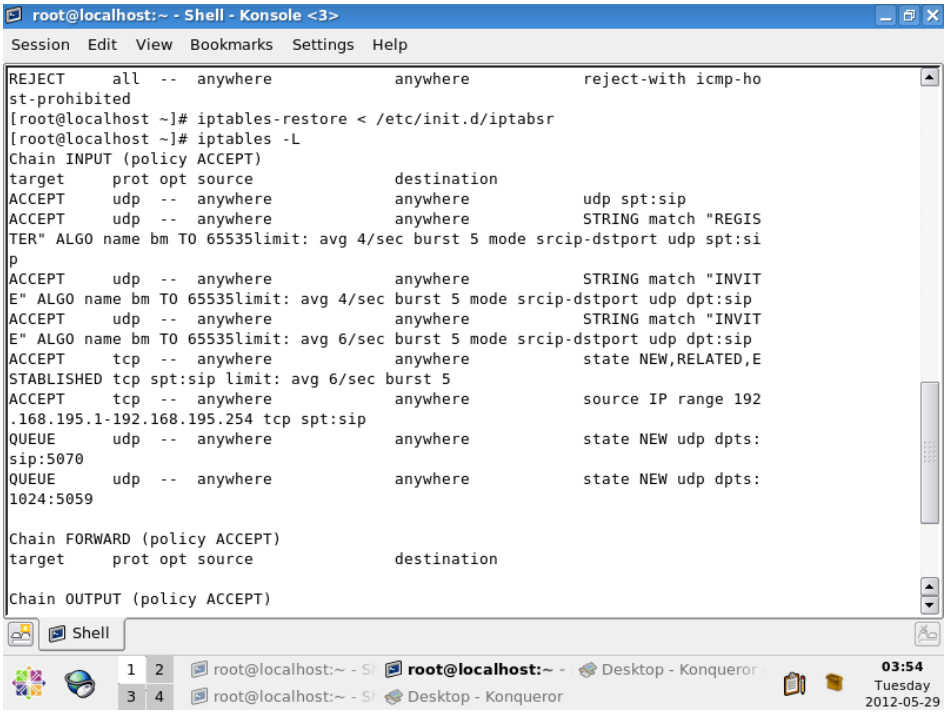


Figure 4.12 IPTable rules to stop inviteflood

This was all about the inviteflood attack and their security to stop the attacks. There are some more attacks that can happen on asterisk like authentication attacks and many more. The Digest Access Authentication (DAA) is currently the most common authentication mechanism for SIP. DAA is simple but rather insecure. It is the only authentication - mechanism which support in SIP is mandatory. DAA uses the MD5 hash function and a challenge-response pattern, and relies on a shared secret between client and server within a SIP domain [38]. The UA receives a nonce value from the SIP server, computes a digest hash value over the nonce, the shared secret and some other SIP header values, and send it to the SIP server. The SIP server computes the same digest hash. If both digests are identical, the UA is authenticated. The DAA is weak and vulnerable to a serious real-world attack [39]. Here is some brief introduction to dictionary attacks and their preventive measures to stop dictionary attacks.

4.7 Dictionary Attacks

An intruder is able to guess poorly chosen passwords by an offline brute force iteration through a *dictionary*, using messages previously collected on the network to verify his

guess at each step dictionary attack. In this, it is taking help of hash values captured by **SIPDump.** These hash values are generated by MD5 hash algorithms. To crack the password, here is a need to capture the SIP authentication digest response. That is done by SIPDump. It is shown in Figure 4.13 as

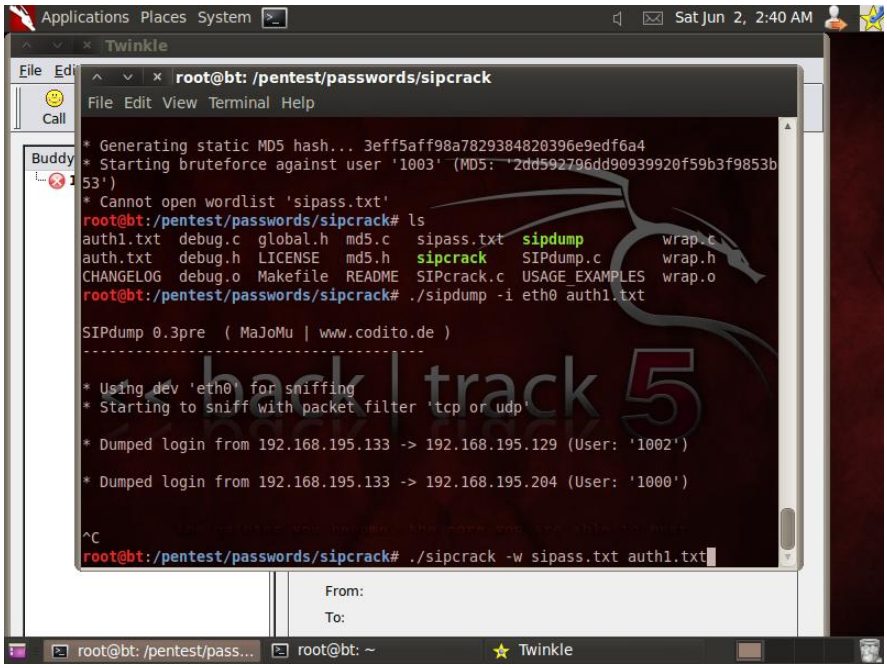


Figure 4.13 SIPDump

It has given some hash values. After getting hash values of the different user logins, get the possible combinations of the words using crunchs. Crunches are used to generate wordlist. Wordlist has been generated by CRUNCHS. **SIPCRACK** is a tool used to do brute force of the digest. Pass those combinations to authentication file and SIPcrack helps in cracking the passwords. It is shown by Figure 4.14 and 4.15

Figure 4.14 Using crunchs to generate wordlist

Time taken by different passwords is different and it depends upon the strength of the password.

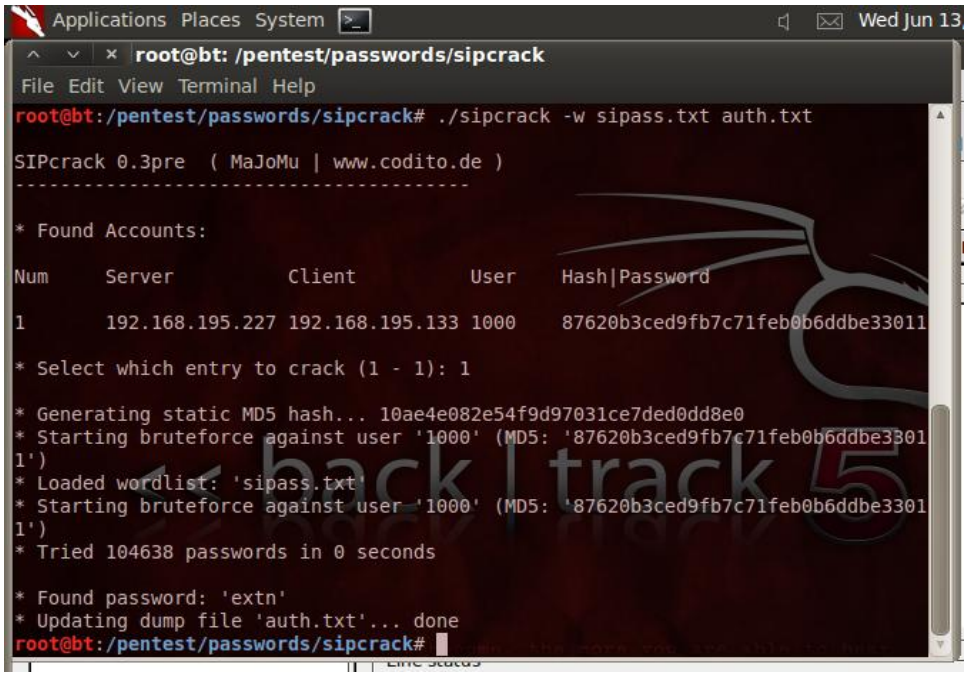


Figure 4.15 Password cracking using SIPCrack

4.8 Problems in MD5

SIP uses a challenge response mechanism to authenticate certain types of requests in particular REGISTER and INVITE requests. Response field contains the 128 bit MD5 hash. MD5 algorithm was invented in 1991 and since that time it has been subject to extensive scrutiny and a number of weaknesses have been found and that was publically declared by United States Computer Emergency Readiness Team (US-CERT) in December 2008. Brute force attack against MD5 hashes with different sized passwords was done on Amazon's EC2 infrastructure using different testing tools like SIPCrack, John the Ripper. The results obtained after brute force attack are shown in Table 4.2

Table 4.2 MD5 Brute Force [40]

Character Set	**Password Length**	**Passwords Attempted**	**Time (s)**	**Time(s) /Password**
Lower case alphabetic	6	321,272,406	251	7.81e-7
Lower case alphabetic	7	2,548,193,457 (test stopped early when password found)	1987	7.79e-7
Alpha numeric and ! $%~-. _#@/?'^(+;,)=[]:><"\{`|}.	5	1,587,031,810	1261	7.74e-7
All 95 printable ASCII characters.	4	82,317,121	64	7.77e-7

Using the assumption that an attacker will be interested in brute forcing a SIP digest for anything under $100 the minimum lengths for a SIP password are listed below and shown in Figure 4.16

- For a password that only uses lower case alphabetic characters a length of 9 characters is required,
- For a password that uses alphabetic, numeric and a select few other ASCII characters a length of 7 characters is required,

- For a password that uses characters that cover the printable ASCII range a length of 6 characters is required.

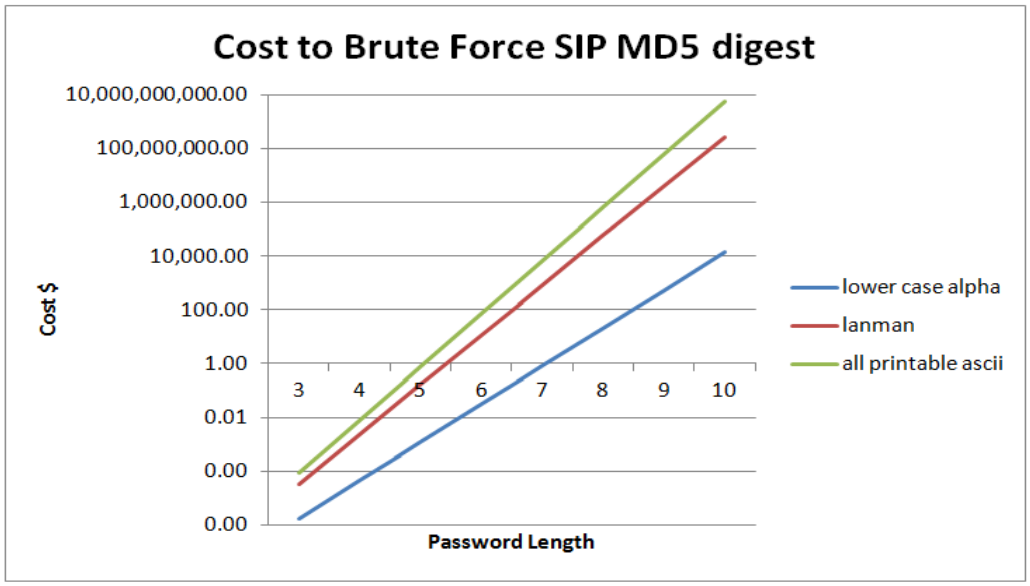


Figure 4.16 Graph for MD5 Brute Force [40]

4.9 S/MIME AND TLS

SIP supports two types of encryption: one is hop by hop and other is end to end. End to end encryption provides confidentiality throughout the message and hop by hop provides security of header fields. End to end security is provided by S/MIME mechanism. It works at application layer of OSI model and hop by hop security is provided by TLS. It works on transport layer and provides transport layer security. S/MIME provides both confidentiality and integrity.

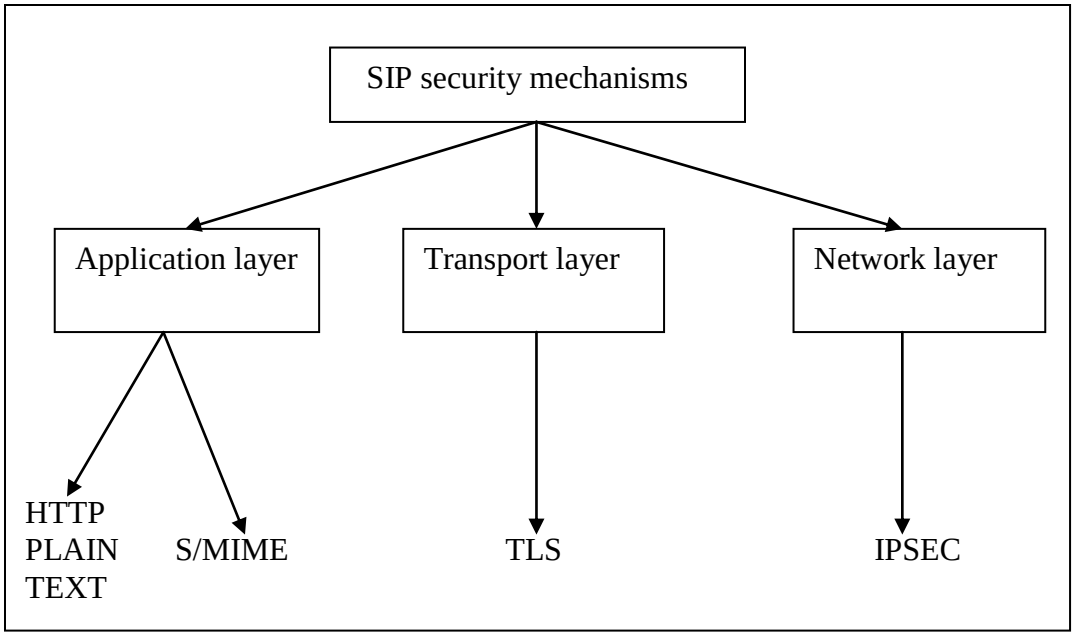


Figure 4.17 SIP Security Mechanisms

S/MIME [41] can be used to secure MIME bodies either on a hop-by-hop basis or end-to-end from user agent to user agent. SIP security mechanisms are shown in Figure 4.17. According to RFC 3261, bodies are signed with the private key of the sender and bodies are encrypted with the intended recipient. MIME body part that has been enhanced acc. to PKCS-7. The application/pkcs7-mime binary enveloped Data structure encapsulates the symmetrically encrypted SDP payload and also contains the symmetric key which is encrypted with the public key of the recipient. The signature plus optionally the X.509 certificate of the signer is contained in the binary application/pkcs7-signature structure which is attached after the MIME object to be signed. This is used to transport both the data to be signed and the signature within a single attachment. TLS works in the same way as HTTPS. It authenticates and encrypts the message on a transport layer.

5. CONCLUSIONS

In order to replace PSTN, SIP based VoIP infrastructure must achieve the same level of reliability, availability and security as in PSTN. In order to contribute to this goal, this thesis investigated the SIP security issues and implemented the security mechanisms for SIP using virtual environment utilizing VMware workstation, asteriskNOW as freepbx and Backtrack 5 R1.

In this thesis, security mechanisms are designed, implemented and deployed for inviteflood attacks and dictionary attacks in SIP. Inviteflood attacks were done using inviteflood tool and controlled using layer 7 firewall i.e. IPTables.

Information gathering, extensions enumeration and fingerprinting to hack SIP network was done using sipvicious tools like SIPDump, smap, svmap and svwar. This information helped in Dictionary attacks to crack the passwords and it also proved the weak digest authentication of SIP i.e. MD5 hash algorithm. To give better protection to SIP protocol S/MIME and TLS were used. S/MIME is used for end-end protection and TLS is used for hop-hop protection. This helped in secure transfer of data.

6. FUTURE SCOPE

SIP is the most prominent protocol that is used in VoIP due to its variety of features, services and advantages as compared to other protocols. But it is very much vulnerable. In this thesis various security issues of SIP are discussed and security mechanisms have been implemented and deployed. It has been proved in this thesis that MD5 algorithm has weak digest authentication access. In future improvements can be done on hashing algorithms that are used for digest authentication. SHA-128 or SHA-256 can be used for stronger digest authentication. For more secure architecture of SIP S/MIME, TLS and IPSEC can be used together at different layers.

REFERENCES

[1] Marius Herculea, Tudor Mihai Blaga and Virgil Dobrota, "Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture", Technical University of Cluj-Napoca, 2008.

[2] Dongwon Seo, Heejo Lee and Ejovi Nuwere, "Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models", in IFIP International Federation for Information Processing, vol. 278, pp. 397-411, 2008.

[3] Butler Barry, "VoIP Services Deep Impact, whitepaper", Juniper Research, March 2006.

[4] Setup IP PBX for small business step by step available at http://www.myvoipapp.com/docs/faq/setup_ippbx_for_small_business_step_by_step/index.html

[5] Samuel Sotillo, "Zfone: A New Approach for Securing VoIP Communication", ICTN 4040, Spring 2006.

[6] Wenyu Jiang, Jonathan Lennox, Henning Schulzrinne and Kundan Singh, "Towards Junking the PBX: Deploying IP Telephony", ACM 1-58113-370-7/01/0006, 2001.

[7] PBX available at http://www.whatispbx.org accessed on 10 may, 2012.

[8] http://www.techknowpartners.com/collateral/whyippbx.pdf accessed on 5 April, 2012.

[9] IP PBX available at http://www.silicon-press.com/briefs/brief.ippbx/brief.pdf accessed on 20 April, 2012.

[10] Network Convergence available at http://searchnetworkingchannel.techtarget.com/ definition/network-convergence accessed on 20 May 2012.

[11] Paul Mahler, "VoIP Telephony with Asterisk", ISBN 09759992-0-6, 2004.

[12] Gomillion David, Dempster Barrie, "Building Telephony with asterisk", ISBN 1-904811-15-9, Packt Publishing Ltd., July 2006.

[13] Qi Qiu, Robert L. Probert, "Study of Digest Authentication for Session Initiation Protocol", University of Ottawa, Dec. 2003.

[14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler,"SIP: Session initiation protocol" Request for Comments 3261, June 2002.

[15] D.Comer, "Computer and Networks with Internet applications", Pearson Prentice Hall, 2003.

[16] Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas, Costas Lambrinoudakis, Stefanos Gritzalis, "SIP Security Mechanisms: A state-of-the-art review", University of the Aegean, Greece, 2004.

[17] Pavel Segec, Tatiana Kovacikova, "A survey of open source products for building a SIP communication platform", University of Zilinia, Advances in multimedia, 2011.

[18] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[19] Jiangbo Yin, "Session Initiation Protocol Benchmark Suite", Delft University of Technology, 2004.

[20] Patrick Crowley, Mark A. Franklin, Haldun Hadimioglu, and Z. Peter, "Network processor design-issues and practices", Morgan Kaufmann Publishers, vol1, 2003.

[21] Mudassir Fajandar, "Implementing an Authorization model in a SIP User Agent to secure SIP sessions", Bombay University, 2000.

[22] Pauli Vesterinen, "User authentication in SIP", University of Technology, 2006.

[23] Ming-Yang Su1 and Chen-Han Tsai2, "A Prevention System for Spam over Internet Telephony", Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, Taiwan, January 2012.

[24] Dimtris Geneiatakis, Tasos Dagiuklas, Georgios Kambourakis, CostasLambrinoudalis and Stefanos Gritzalis, "Survey of Security Vulnerablities in SIP", IEEE, vol 3, 2006.

[25] Flavio E. Gonçalves, "A step-by-step guide to building a simple IP PBX", V.Office Networks, November 2006.

[26] AsteriskNOW available at http://www.asterisk.org/asterisknow accessed on 10 Feb 2012.

[27] Jim Van Meggelen, Leif Madsen and Jared Smith, "Asterisk the Future of Telephony", O'Reilly Media, Aug 2007.

[28] Leif Madsen, Jim Van Meggelen and Russell Bryant, “Asterisk-The Definitive Guide 3rd edition”, 2011.

[29] Lehtinen, R., and G. T. Gangemi, “Sr. Computer Security Basics”, O'Reilly, 2006.

[30] Gaston Ormazabal , Sarvesh Nagpal , Eilon Yardeni , Henning Schulzrinne, “A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems”, Proceedings of the 2nd International Conference on Principles, Systems and Applications of IP Telecommunications, Springer, pp. 107-132, 2008.

[31] W. Werapun, A. Abou EI Kalam, B. Paillassa, and J. Fasson, “Solution Analysis for SIP Security Threats”, University of Toulouse, IEEE, 2009.

[32] Thandry, N., Pendse, R., and Namuduri, K., “Voice over IP Security and Law Enforcement,” Proceedings of the 39th International Carnahan Conference on Security Technology (ICCST), pp. 246-250, Las Palmas de Gran Canaria, Spain, Oct. 2005.

[33] David Butcher, Xiangyang Li and Jinhua Guo, “Security Challenge and Defense in VoIP Infrastructures”, IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, vol. 37, no. 6, November 2007.

[34] Abhishek kumar, Dr. P. Santhi tilagam, “A novel approach for evaluating and detecting low rate SIP flooding attack”, international journal of computer applications, vol. 26, July 2011.

[35] X-LITE available at http://www.counterpathcorporation.com.

[36] Twinkle available at http://mfnboer.home.xs4all.nl/twinkle/index.html.

[37] Stateful Firewalls available at http://www.pearsonhighered.com/samplechapter/0672327376.pdf .

[38] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," RFC 2617 (Draft Standard), Internet Engineering Task Force, Jun. 1999. [Online] Available: http://www.ietf.org/rfc/rfc2617.txt, Apr 2012.

[39] L. Strand and W. Leister, "Improving SIP authentication," in Proceedings of the Tenth International Conference on Networking (ICN2011), Xpert Publishing Services, pp. 164 – 169, Jan 2011.

[40] MD5 Brute Force available at http://www.sipsorcery.com/mainsite/Help/SIPPassword Security, accessed on 25 May 2012.

[41] Ramsdell B, S/MIME Version 3 Message Specification, IETF RFC 2633, 1999.

List of Publications

"Design, Implement and Deploy Security Mechanisms for Session Initiation Protocol", Sheetal, Maninder Singh, "International Journal of Computer Applications", communicated, July 2012.