Spam Detection and Prevention Framework Over Internet Telephony

By

Nirav V. Panchal

08MCE007

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May 2010

Spam Detection and Prevention Framework Over Internet Telephony

Major Project

Submitted in partial fulfillment of the requirements

For the degree of Master of Technology in Computer Science & Engineering

By

Nirav V. Panchal

08MCE007

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

AHMEDABAD-382481

May 2010

Declaration

This is to certify that,

i) The thesis comprises my original work towards the degree of Master of Technology in Computer Science and Engineering at Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

- Nirav V. Panchal
08MCE007

Certificate

This is to certify that the Major Project entitled ”Spam Detection and Prevention Framework Over Internet Telephony” submitted by Nirav V. Panchal(08MCE007), towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering of Nirma University of Science and Technology,Ahmedabad is the record of work carried out by him under my supervision and guidance.In my opinion,the submitted work has reached a level required for being accepted for examination.The results embodied in this major project,to the best of my knowledge,haven't been submitted to any other university or institution for award of any degree or diploma.

Dr. S.N. Pradhan
Guide, PG-Coordinator,
Department of Computer Engineering,
Institute of Technology,
Nirma University, Ahmedabad

Prof. D. J. Patel
Professor and Head,
Department of Computer Engineering,
Institute of Technology,
Nirma University,Ahmedabad

Dr K Kotecha
Director,
Institute of Technology,
Nirma University,Ahmedabad

Abstract

Spam Over IP telephony is considered to be a threat in communications and it has the potential to become even more annoying than E-mail spam because recipients will be disturbed by each received spam.So exploring the properties of spam from conversations to detect them and use these properties to prevent spam before interrupting users.Due to live communication nature of VOIP,the time available to filter and analyze the VOIP spam is very less as compared to the time available to detect E-mail spam. The aim of this dissertation work is to propose a framework which will able detect and prevent the spam (SIP invite flooding via unregistered user). This approach helps to improve the Quality-of-Service(QOS) of legitimate users during the SIP flooding attack.

This report contains, a general overview of Spam, VOIP spam and its comparison with E-mail spam, analytical survey of existing AntiSPIT frameworks as well as study and implementation of SPIT generation(SIP invite flooding via unregistered user). The implementation of AntiSPIT framework, experimental work and analysis of results based on the Quality-of-Service parameters are discussed.

Acknowledgements

Before,I get into thick of things I would like to add a few heartfelt words for the people who were part of my thesis in numerous ways,people who gave unending support right from the beginning.During this period, the faculty members and my batch mates took keen interest and participated actively.They are very efficient and qualified in their respective disciplines.

I express my sincere gratitude to my thesis guide **Dr.S.N.Pradhan**,M.Tech Coordinator,Computer Science & Engineering Dept.,Nirma Institute of Technology,Nirma University who suggested many related points and always very constructive and helpful for all his affectionate encouragement and guidance during the entire thesis.His views and inputs are very helpful throughout the process.

I would like to thank **Dr. Ketan Kotecha**,Director, Nirma Institute of Technology,Nirma University for the facilities and environment for research.

At last but not least, I would like to appreciate the support and suggestions of my dear friends **Mr.Shailesh Panchal and Mr.Paresh Solanki** who continuously encouraged me during the progress of my thesis work.

Lastly,I would like to thank my family for their love,support and encouragement that they have given me throughout my life and helping me to persevere in my studies.

- Nirav V. Panchal
08MCE007

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The explosion of the Internet has generated a wide array of technological advances related to packet-switched data networks.Development in data networks has occurred more quickly than the traditional telephony circuit switched network.As a result,and with the growth of broadband connectivity,it is becoming more reasonable for businesses and consumers to communicate through their Internet connections as opposed to their traditional telephone carrier networks[1].

VOIP technologies take advantage of existing data networks to provide inexpensive voice communications worldwide as an alternative to the traditional telephone service.There are many advantages to VOIP including cost savings, open standards and integrated networks.VOIP applications provide cost savings as they reduce their reliance on the Public Switched Telephone Network(PSTN)and only require maintenance of one network of intermixed voice and data.

Voice over IP (VOIP)uses the Internet Protocol(IP) to transmit voice as packets over an IP network.Therefore,VOIP can be achieved on any data network that uses IP like the Internet,Intranets and Local Area Networks(LAN).Using VOIP,voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls,carry information required to locate users, and negotiate capabilities.The Session Initiation Protocol(SIP)is an application-layer signaling-control protocol used to establish,maintain,and terminate multimedia sessions. Multimedia sessions include VOIP, conferences and other similar applications involving such media as audio,video and data.

Spam is defined as the transmission of bulk unsolicited mails.It is considered to be one of the biggest problem the internet has ever faced.With the increasing deployment of Internet telephony solutions,often referred to as VOIP,it is commonly expected that a similar form of spam will affect also this area.This threat is known as SPIT and it is defined as the transmission of unsolicited calls or invite messages over Internet Telephony[1, 2].

1.1 Objective

There are two major types of SIP-based VoIP deployment : VoIP on a purely private network and VOIP on an open Internet.When VOIP is deployed on a purely private network,it is normally highly integrated with a PSTN network and VPN where users cannot access the system from outside.This can protect the system from external attacks,however it cannot stop attacks from the internal network.If this system is deployed as a public service,and can be accessed via the the internet,it is susceptible to flood attacks from both internal and external users.Even though the topological implementations are different on the different types of SIP-based VoIP deployment,the attack mechanism and impact are similar in both systems.

The objective of this dissertation work is to find a solution to mitigate SIP flooding attacks,which is able to drop the majority of attack packets to provide a good Quality-of-Service parameters for legitimate users[2].

1.2 Organization of work

- Study papers on SPIT(Spam over internet telephony),VOIP Quality-of-Service parameters,comparison between SPIT and E-mail spam,AntiSPIT frameworks and their countermeasures as well as Existing SIP flooding attack mitigation methods.
- Study and configure VOIP lab using SIP based Open source Softphone which works as Client and Open source PBX which works as Server.
- Study and Implementation of manually spam(SIP invite traffic)generation.
- Implementation of AntiSPIT framework which mitigates SIP invite flooding to maintaining a good Quality-of-Service for legitimate users.
- Analysis of experimental results based on Quality-of-Service parameters for legitimate users as per proposed antiSPIT frameworks.

1.3 Outline of Thesis Report

The rest of the thesis is organized as follows.

Chapter 2, gives a detail literature survey related to VOIP spam,VOIP Quality-of-Service parameters, comparison between SPIT and e-mail spam,existing Anti-SPIT frameworks thieir countermeasures as well as Existing SIP flooding attack mitigation methods.

Chapter 3, describe the detail study and configuration of VOIP lab using open source softphone which works as VOIP client and open source PBX which works as VOIP server.

Chapter 4, describe the detail study and implementation of manually Spam(SIP invite traffic)generation which works as Spitter.

Chapter 5, describe the detail design and implementation of proposed Spam detection and prevention framework.

In **Chapter 6**, experimental results and analysis are presented.

Finally, in **chapter 7** concluding remarks and scope for future work is presented. Materials (e.g.URLs and research papers) used and studied are given in References.

Chapter 2

Literature Survey

This chapter gives a detail literature survey related to VOIP spam,Quality of Service(QoS)parameters,comparison between SPIT and e-mail spam,existing AntiSPIT frameworks and their countermeasures as well as Existing SIP flooding attack mitigation methods.

2.1 Spam

Spam is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.Spam flood the Internet with many copies of the same message.Spam waste network bandwidth and time of recipients.Spam is also profitable by sending it to recipients in form of advertising message[1].

2.2 VOIP Spam

SPIT [1, 2, 3]is defined as "transmission of bulk unsolicited messages and calls".It doesnt characterize the content and also include messages.If the term "messages" is use then its called SPIM (SPAM over Instant Messages)."Call SPAM" is defined as "a bulk unsolicited set of session initiation attempts"(e.g,"SIP invite" requests attempting to establish a voice,video,instant messaging).

2.2.1 VoIP Quality of Service(QoS)parameters

VoIP faces two challenges which are more serious than in traditional PSTN networks: quality of service and security.Owing to the fact that in VOIP networks there is typically a great deal of infrastructure resource sharing, the quality of a VoIP network cannot be guaranteed to the same extent as in the PSTN network.Service quality on a VoIP network consists of the following factors: Network Availability,Latency,Jitter and Packet Loss.This project is to be focus on two factors: Network Availability and Latency.Call setup delays is be measured as the main system performance factor.Call setup delay indicates the time takes to setup a phone call.This can reflect the latency of the network during the call setup phase,and the call setup timeout rates can indicate the network availability.

2.2.2 Basic categories of SPIT

These are the basic categories of SPIT [5]:

- SPIT is sent on-path associated with SIP signaling.The SPIT sent through a normal signaling route by a spammer who registered to the VoIP service(Normal means Telemarketers as a spammer who have already registered to the VoIP service and send the SPIT message.

- SPIT sent off-path associated with SIP signaling.The SPIT sent through an abnormal signaling route by a spammer who did not register to the VoIP service(Abnormal means that a spammer who did not register to the VoIP services tries to send the SPIT message using dictionary attack or sniffing.

2.2.3 VOIP Spam vs. E-Mail Spam

SPIT contains the phrase ”SPAM” and has some parallels with E-mail spam.E-mail spam(communicate asynchronously)and SPIT(communicate asynchronously and synchronously).E-mail arrives at the E-mail server before it is accessed by the user.

This means that structure and content of an email can be analyzed at the server before it arrives at the recipient and So, SPAM can be detected before it disturbs the recipient while SPIT uses real-time communication and its must require to analysis during session establishment or during session[2].

2.2.4 SPIT Initiator

The initiator of SPIT has the goal to establish a communication session with as much victims as possible in order to transfer a message to any available endpoint.They can fulfill this based on three steps which are given below[5]:

- Information Gathering : If an attacker wants to reach as many victims as possible,he must catalogue valid assigned SIP URIs.The premisses for the Scan attack are the possession of at least one valid account and knowledge about the scheme of SIP URIs of the targeted platform.
- Session Establishments : When the attacker has collected a large number of contact addresses, he can begin session establishment to the victims.The attacker can establish a session with sending an INVITE message via Proxy, which we can call SPIT via Proxy or he can establish a session with sending an INVITE message directly to the endpoint without involving the Proxy.
- Send Messages : The last step of the SPIT initiator is the media sending after the session has been established.Which type of media is sent depends on the scenario in which the SPIT attack takes place.

2.2.5 SIP Threat Assessment Summary

SPIT threat work as the possible action or event that exploits SIP vulnerabilities in order a SPIT attack to be conducted.Therefore,AntiSPIT mechanism should minimize the recognized threats by eliminating vulnerabilities regarding SPIT.

The following threats received high likelihood or impact valuations and it should also be taken into account by an Anti-SPIT mechanisms[2]:

Exploitation of invite Messages,Exploitation of Request Messages,Sending Ambiguous Requests to Proxies,Contacting a redirect server with ambiguous requests, Throwaway SIP accounts,Exploitation of Headers Fields(Error-Info),Exploitation of registrar servers.

2.3 Antispam Frameworks And Countermeasures

SPIT handling should be conducted in three progressive steps given below to required for an efficient management of this phenomenon.
(a) Prevention(To stop SPIT)
(b) Detection(To detect a SPIT call or message)
(c) Handling SPIT call or message.
These are the basic three kinds of methods to detect the spam[4]

- Non-intrusive methods are based on the exchange and analysis of signaling messages. They do not create inconveniences for the caller and they do not disturb the callee, if they block SPIT calls successfully. The effectiveness of such methods is limited and not expected to be sufficient. This kind covers blacklisting,detections of call rates,call patterns,reverse lookup of caller DNS entries.

- Caller interaction methods that create inconveniences for the caller by requesting him/her to pass a checking procedure for the call which is typically based on question and answer or more general on action and reaction checking.

- Callee interaction methods that exchange information with the callee on a per-call basis. These methods are problematic, because they might miss the general goal of protecting the callee from disruptions.

2.4 Anti-Spam Techniques based on the E-mail spam paradigm

Brief description of the general anti-SPIT frameworks based on the email spam paradigm, aiming to classify them according to the above basic three kinds of progressive steps[2].

2.4.1 Black and white lists

White lists contain trusted users that are not classified as spitters. An end-used accepts the calls,or messages,initiated by any of the members in white list.On the other hand,black lists include the potential initiators of SPIT calls.These calls should be blocked.

2.4.2 Content filtering

It is based on filters that check the contents of messages. They appear to be inappropriate as anti-SPIT,since real-time filtering is hard to be done.This technique could be used only for the detection of instance messaging SPIT.

2.4.3 Reputation-based

The approach is based on the notion of trust. When a callee receives a request for communication the level of trust of the caller should be determined.If the trust level is above a predefined threshold then the communication is permitted,otherwise it is rejected.

2.4.4 Charging-based

This approach forces spitters to pay for every unsolicited bulk call.The goal of this method is to inform the sender that he/she should pay a fee in order the request to be satisfied.If the sender refuses payment,the SIP session is to be terminate.

Table I: Antispam Framework Countermeasures based on Email spam paradigm

Mechanism	*Prevent*	*Detect*	*Handle*
Black and white lists	no	yes	no
Content filtering	no	yes	yes
Reputation-based	yes	yes	no
Charging-based	yes	yes	no

2.5 Anti-SPIT methods and their Countermeasures

2.5.1 Network-Level Anti-SPIT Entity

The role of this entity is to filter and analyze the network traffic.[2] The analysis is performed on the transmitted SIP packets, and the detection of SPIT depends on five criteria,namely (a)The duration of the calls (b)The number of received error messages returned from SIP protocol,(c)The automated logic of addresses presented in SIP headers,(d)The simultaneous calls attempts and (e)The analysis of the simultaneous calls made by a user. By using these criteria, a weighed sum is introduced,namely SPITLevel, which serves as a threshold.If the SPITLevel is exceeded the call is classified as SPIT.

2.5.2 Progressive Multi Gray-Leveling

The PMG calculates and assigns a gray level for each caller in order to check if a message is SPIT or not. Gray level indicates a label between white and black, and is used for the determination about the legitimacy of a sender. This level is calculated based on previous call patterns of the particular caller, rather than the feedback from other users.

2.5.3 Differentiated SIP

It tries to handle SPIT through the classification of callers into three categories of lists, namely: white, who are legitimate callers, block, who are spitters, and grey list, who are not yet classified as legitimate callers or spitters. Through this classification the handling of calls is conducted differently, according to the caller's categorization. More specifically, when a caller belongs to the callee's whitelist then the call could be established. When the caller belongs to the callee's blacklist then the call is rejected. When the caller is unknown,then the caller should pass a human verification test.After passing the test the caller is free to communicate with the callee.

2.5.4 Voice Spam Detector

VSD are the following filters:(a)presence,(b) traffic pattern,(c) black and white lists (d) Bayesian learning and (e) social networks and reputation. Presence filtering.VSD checks for any recorded SPIT behavior associated with any of the participating entities, by looking up trust information available for those entities. The trust information would be available if any of the entities has a history of calling an end-user. Finally,reputation techniques are used to check the acceptance of a call based on social relationships (network) that an end user maintains with other entities participating in the VoIP environment.

Table II: AntiSPIT Framework Countermeasures

Mechanism	*Prevent*	*Detect*	*Handle*
Network-Level Anti-SPIT Entity	no	yes	yes
Progressive Multi Gray-Levelling (PGM)	no	yes	yes
Differentiated SIP	no	yes	no
Voice Spam Detector	yes	yes	no

2.6 SIP flood attacks and existing countermeasures

SIP flood attacks are the major threat to VoIP systems.A SIP message flooding attack occurs when an attacker sends a large number of INVITE or REGISTER requests with spoofed source IP addresses.It is worth pointing out that even though there are many other types of SIP requests,INVITE and REGISTER are the predominant messages used by SIP and they require more processing at the SIP components than all the other requests.Thus,SIP-based VOIP systems are especially vulnerable to flooding attacks using these SIP invite flooding[7].

2.6.1 Impacts of SIP flooding attack

There are two major impacts resulting from a SIP flooding attack:

- Memory exhaustion: When a SIP proxy server receives a SIP request(REGISTER or INVITE) it needs to copy each incoming request into its internal buffers to be able to process the message which makes the proxy server vulnerable to memory exhaustion attacks.

- CPU exhaustion: After the incoming requests are saved, the SIP proxy server will process (authentication or destination address look-up etc.)the requests and generate and send responses.The CPU resource can become highly loaded if a large number of requests are flooded at the SIP proxy server.

- Link Bandwidth: SIP flooding attacks can exhaust the link bandwidth of the SIP proxy server and cause a denial of service at the access point to the VoIP system.

2.6.2 Existing SIP flooding attack mitigation

- Firewall: Implementation of a firewall is the most common security technique used to protect network components from external attacks.Traditional firewalls use layer-3 filters to block unwanted traffic while some modern firewalls use application-layer gateways based on layer-7 filtering.Firewalls are generally designed for general purpose traffic filtering and will often not detect application-specific attack traffic[8].

- Intrusion Detection: It helps to spot attack traffic at real-time,so further anti-flood mechanisms can be triggered to stop the attacks and It does not provide mechanisms to stop the attack traffic.
- Intrusion Prevention: The most commonly used techniques in SIP intrusion detections are: a state machine-based detection engine, and a request header examine engine.The advantage of SIP intrusion detection mechanisms is that they do not typically require collaboration of a large number of hosts,which makes the implementation easier.

None of the framework examine the content of the SIP messages and do not adequately detect and handle SIP threats.Even the content filtering framework that checks the main bodies of messages, cannot mitigate these threats and it is not signaling but media oriented. Specifically it does not check the messages that are in charge for session and call management.In the case of SIP base VOIP spam handling frameworks also does not check actual content of the calls.As a step for Anti-spitting, none of the proposed architectures is capable of detecting the identified SIP SPIT threats.Thus,Most of them do not check the messages contents[2].

Thus,conclusion is that none of the existing approaches can help to eliminate the impact of SIP flood attack.So,Propose a new SPIT prevention system which will improve QOS for legitimate users.

Chapter 3

VOIP configuration

This chapter describe the detail study and configuration of VOIP lab using open source softphone which works as VOIP client and open source PBX which works as VOIP server Over LAN.

3.1 Study and Configure VOIP Server

Software base PBX (private branch exchange) system which works as a registrar,proxy and authentication server as well.It manages internal clients by having their state and information at any given time.So when a SPIT is generated it has to go through the PBX server because it doesn't identify the client directly.SPITs are generated and routed through the PBX server to the end points.SPIT detector module can be added as a thin layer which filters outs the SPITs.Asterisk and sipXecs are the open source PBX behind a number of SIP based open source VoIP projects[6].

3.1.1 Difference between asterisk and sipXecs

These are the basic difference between asterisk and sipXecs :

- sipXecs supports only SIP but Asterisk is known to support SIP and H.323 also.

- sipXecs IP PBX does not route calls (media) through the server because it separates signaling from media but Asterisk does route calls through the Asterisk server so it is very useful for AntiSPIT framework implementation.
- Asterisk is written in C. The sipXecs Communications server infrastructure is written in C++.

3.1.2 Asterisk PBX

Asterisk is an open source IP based PBX (private branch exchange) system.It allows communication between remote parties through attached IP phone or traditional phone connecting them. It can also be used as a gateway in case of SIP to connect to other service including public switch telephone network (PSTN). It has many features available as in the normal PBX system such as call forwarding, call waiting, etc.It can act as a registrar, proxy server or redirect server during SIP implementation. Asterisk is completely open source, allowing developers to add new functionality in it[6].

3.2 Basic Configuration Steps of Asterisk

Basic prerequisites[6]:

- The SIP configuration file : SIP.conf
- The extensions file (dialplan) : Extensions.conf

3.2.1 Dial plan

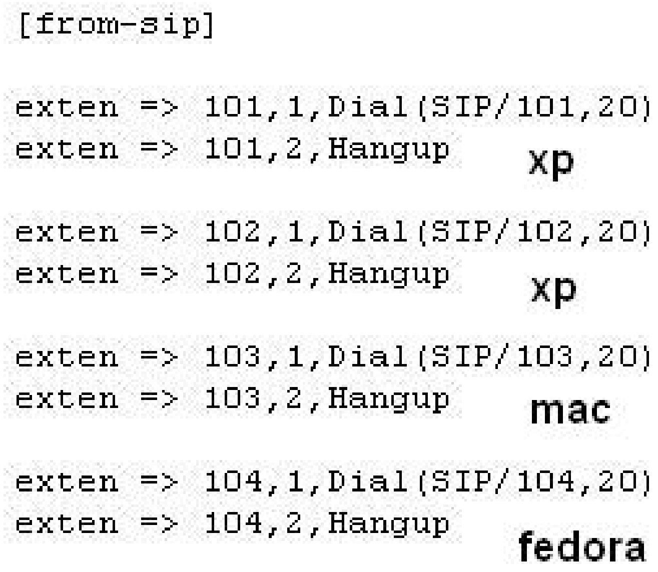
A dialplan is the logic that instructs Asterisk to handle the calls. The Asterisk dialplan exists purely in software and is predominantly written in the file extensions.conf.This file lays out the dial plan,brings channels together with applications and services.This file resides in /etc/asterisk.

Basic example of Dialplan(extension.conf):

[internal]

- exten 100,1,Answer()
- exten 100,2,Wait(1)
- exten 100,3,Playback(hello-world)
- exten 100,4,Hangup()

Dialplan (Manually configuration):



```
[from-sip]

exten => 101,1,Dial(SIP/101,20)
exten => 101,2,Hangup

exten => 102,1,Dial(SIP/102,20)
exten => 102,2,Hangup

exten => 103,1,Dial(SIP/103,20)
exten => 103,2,Hangup

exten => 104,1,Dial(SIP/104,20)
exten => 104,2,Hangup
```

Figure 3.1: Extension.conf

3.2.2 SIP Configuration file

This file is of importance because it is required for SIP based VoIP phone to access a via asterisk(PBX).This file handles user registration part. After registration,SIP phone can place or receive calls using via asterisk(PBX).This file resides in /etc/asterisk.

Example of SIP extension(sip.conf)given below :

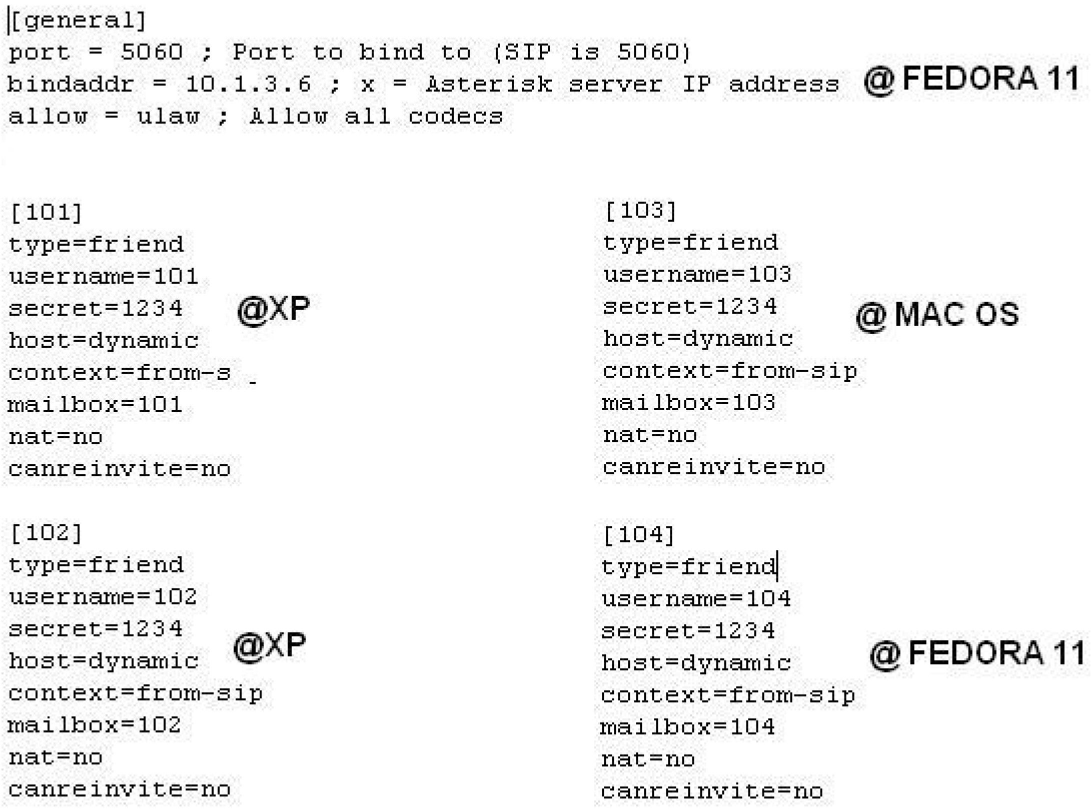
[1001]

- user = 1001
- type = friend
- secret = 1234
- host = dynamic
- callerid = 1001
- context = from-sip-internal

The description of above example given below :

- The "user" identifier is assigned to the extension that is use with softphone.
- The "type" identifier tells the user is a "user" (takes incoming calls),"peer" (makes outgoing calls) or a "friend" (who does both).
- The "secret" identifier is assigned the password for authenticating the user.This has to be accurately entered in the phones configuration settings needed to log on the Asterisk server.
- The "host" identifier tells Asterisk what kind of host which deals with and the value "dynamic".it informs Asterisk that this host will register with server.
- The "callerid" identifier is the caller identification presentation string that is seen by caller.
- context = from-sip-internal

SIP.conf(Manually configuration):



```
[general]
port = 5060 ; Port to bind to (SIP is 5060)
bindaddr = 10.1.3.6 ; x = Asterisk server IP address
allow = ulaw ; Allow all codecs
```

```
[101]
type=friend
username=101
secret=1234
host=dynamic
context=from-s
mailbox=101
nat=no
canreinvite=no

[102]
type=friend
username=102
secret=1234
host=dynamic
context=from-sip
mailbox=102
nat=no
canreinvite=no
```

```
[103]
type=friend
username=103
secret=1234
host=dynamic
context=from-sip
mailbox=103
nat=no
canreinvite=no

[104]
type=friend
username=104
secret=1234
host=dynamic
context=from-sip
mailbox=104
nat=no
canreinvite=no
```

Figure 3.2: SIP.conf

3.3 Study and Configure VOIP Client

A soft phone is a phone that allows to talk using VoIP without necessarily having a physical phone set.Clients are soft phone which can be described as software that generates and establish voice communication over a network or the Internet.A typical soft phone connects to the service provider to call other party over Internet while the other type of soft phones is connected by a software PBX system over local area network. The protocol used by most of the soft phones for VoIP communication is SIP. The clients connected by PBX system consists a small network within themselves largely used within an organization just like conventional PBX system, more ever the large number of VoIP clients are deployed as a hard/soft phone with software based PBX system. VoIP service providers can me modeled as large PBX system which leads to go for detection development on software based PBX system.

3.3.1 Open source Soft phones works as SIP clients

These are open source Soft phones as SIP clients which mostly used in VOIP network:
CounterPath X-Lite,Ekiga,KPhone,minisip,Phoner and Phonet Lite,SIPSet,SJphone, PJphone,Skype,WindowsLiveMessenger,Yahoo Messenger.

These are the best SIP Softphones :

Ekiga(GnomMeeting):

It is One of the best SIP Softphone around in the market today. It supports VoIP and video conferencing using H.323 and SIP protocols.

These are the Features :

It supports many audio and video codecs and is interoperable with other SIP compliant software support for the G.722 audio codec,ENUM support,Transparent NAT Support using STUN and Line Monitoring.

X-lite:

It is widely used SIP softphone in the world. Its easy to use and configure.

These are the Features :

Enhanced Quality of Service for voice and video calls,Multi-party and ad hoc Voice and Video Conferencing,Voice and Video Call Recording,Very Easy Interface for SIP Account Configuration.

KPhone:

It is a SIP User Agent for Linux and also acts as a VOIP/SIP softphone.

These are the Features :

IPv4 and IPv6 support,Multiple parallel sessions,NAT traversal and STUN support,SRTP encryption for voice.

SJPhone:

It supports SIP and is fully inter-operable with most major VOIP vendors.

These are the Features :

It Supports both SIP and H.323,free and paid versions are available.Supports Windows, Linux,Mac OS X,Windows CE.

basic fields SIP account settings

- Display Name.
- User Name.
- Password.
- Authorization User.
- Domain.
- Register with domain and receive incoming calls.
- Send outbound via proxy address.

3.3.2 Configuration Steps for the Softphone

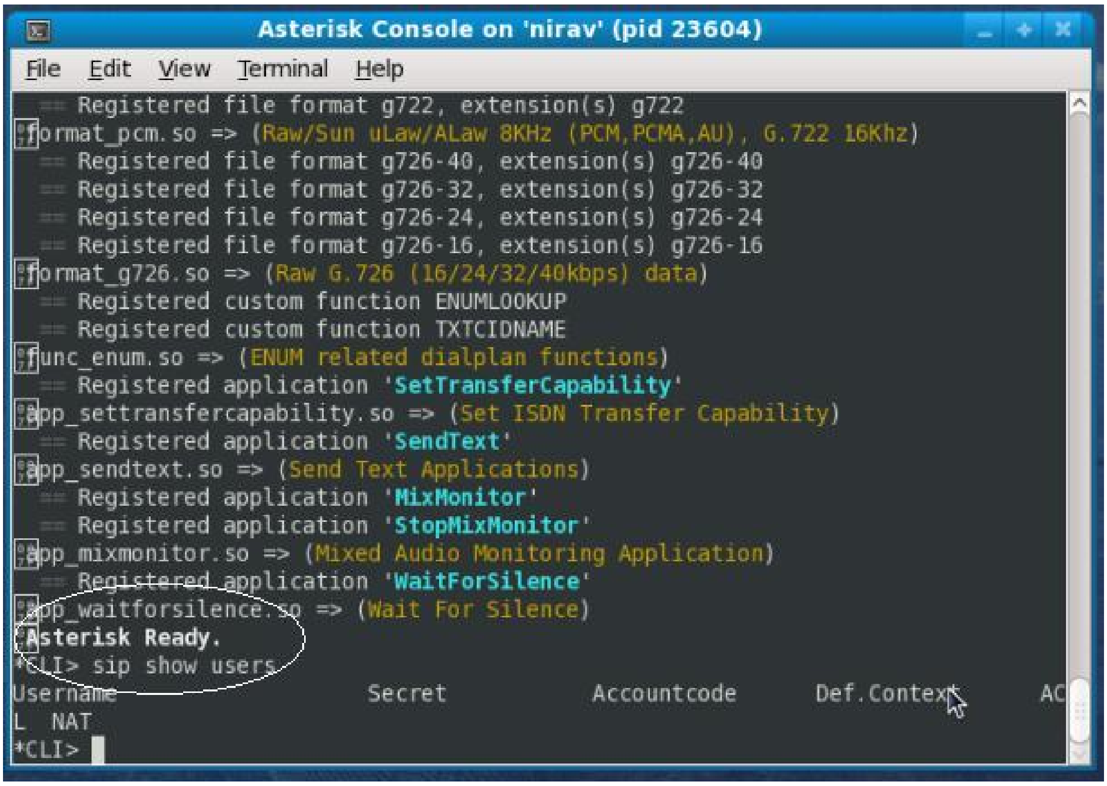
these are the Configuration Steps of Softphone for the connectivity with Asterisk

- Domain: Asterisk machines IP address.
- SIP proxy: Asterisk machines IP address colon separated with your Asterisks SIP port.
- Outbound SIP proxy: SIP proxy for making outbound calls here. Usually this is same as the SIP proxy.
- User name/Authorization user: The extension that is needed to assign the phone.
- Password.

3.4 Clients connections via Server

ASTERISK

After the complete installation of Asterisk in fedora 11,sip show peers or sip show users command give the Status of clients on asterisk console shown below:

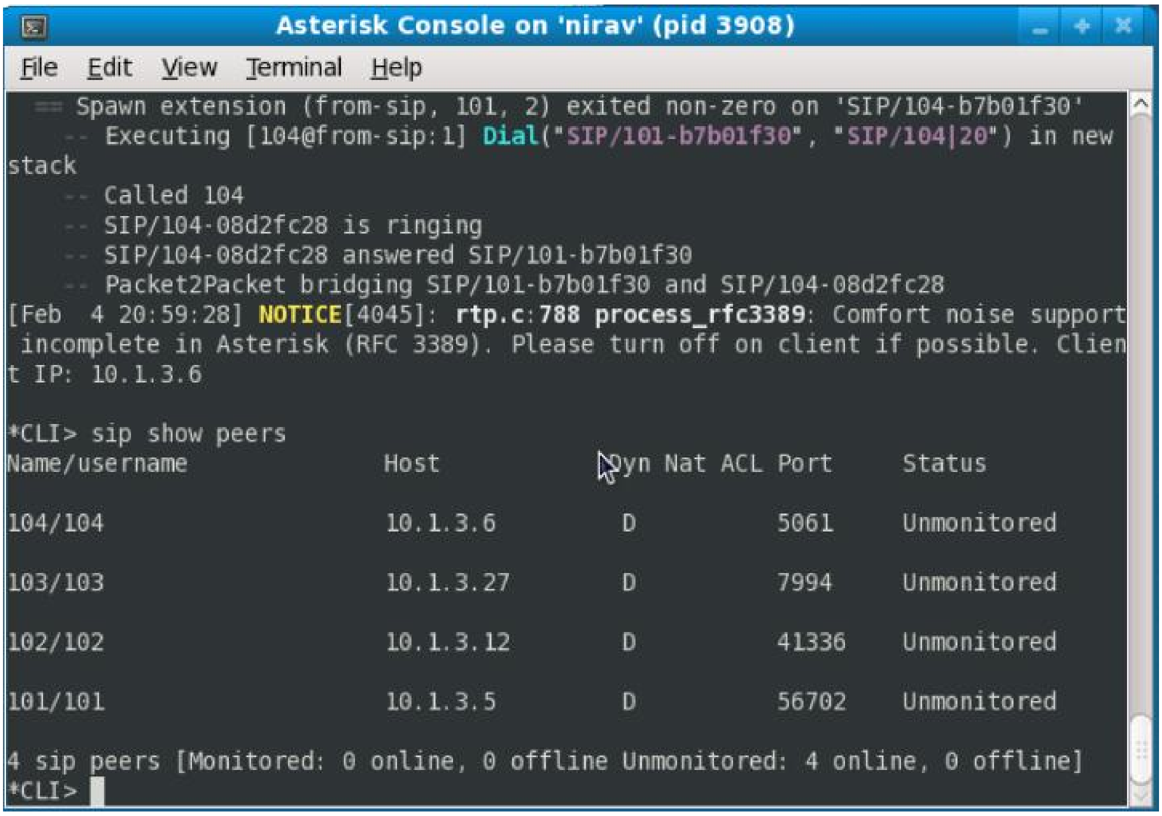


```
  == Registered file format g722, extension(s) g722
format_pcm.so => (Raw/Sun uLaw/ALaw 8KHz (PCM,PCMA,AU), G.722 16Khz)
  == Registered file format g726-40, extension(s) g726-40
  == Registered file format g726-32, extension(s) g726-32
  == Registered file format g726-24, extension(s) g726-24
  == Registered file format g726-16, extension(s) g726-16
format_g726.so => (Raw G.726 (16/24/32/40kbps) data)
  == Registered custom function ENUMLOOKUP
  == Registered custom function TXTCIDNAME
func_enum.so => (ENUM related dialplan functions)
  == Registered application 'SetTransferCapability'
app_settransfercapability.so => (Set ISDN Transfer Capability)
  == Registered application 'SendText'
app_sendtext.so => (Send Text Applications)
  == Registered application 'MixMonitor'
  == Registered application 'StopMixMonitor'
app_mixmonitor.so => (Mixed Audio Monitoring Application)
  == Registered application 'WaitForSilence'
app_waitforsilence.so => (Wait For Silence)
Asterisk Ready.
*CLI> sip show users
Username                   Secret           Accountcode      Def.Context       AC
L  NAT
*CLI>
```

Figure 3.3: Asterisk(PBX)console(without using client's registration)

After the configuration of SIP.conf and Extention.conf files of asterisk ,sip show peers or sip show users command give the information of registered user on its console.

Status on the asterisk console with registered user shown in below:

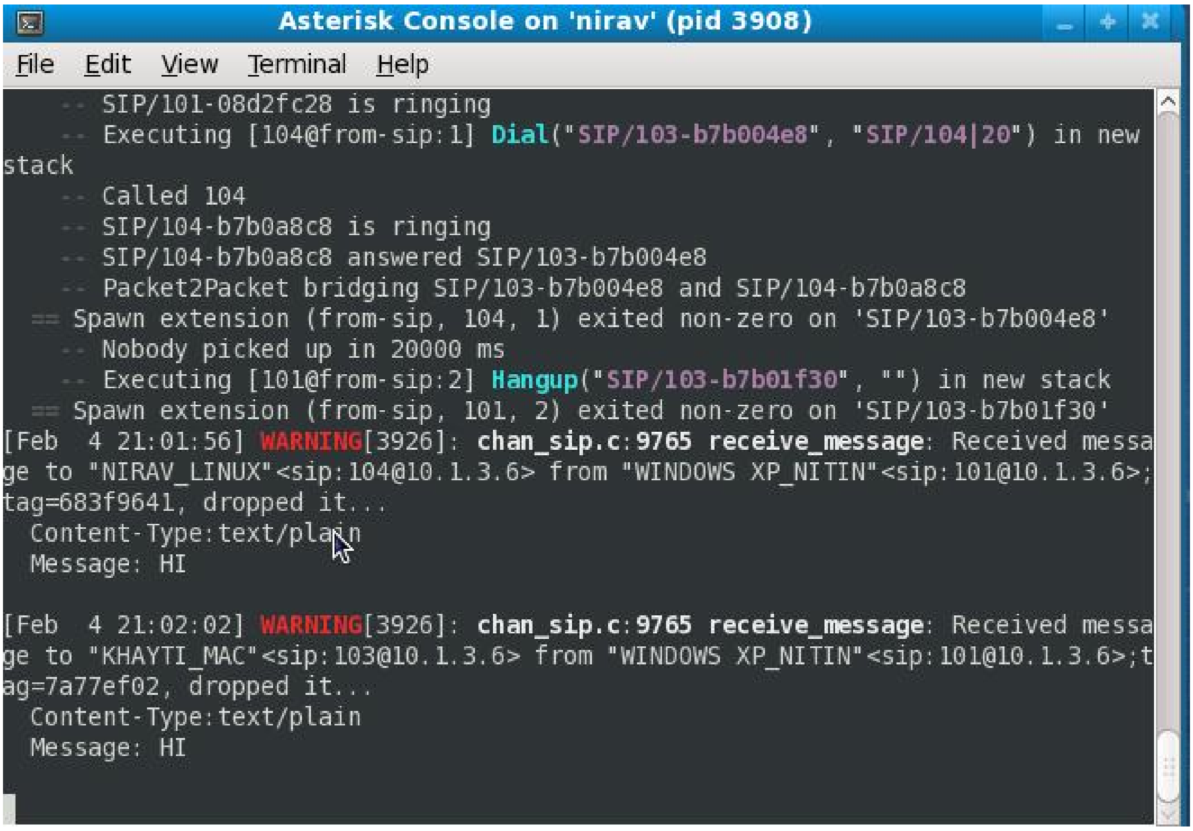


```
    == Spawn extension (from-sip, 101, 2) exited non-zero on 'SIP/104-b7b01f30'
    -- Executing [104@from-sip:1] Dial("SIP/101-b7b01f30", "SIP/104|20") in new
stack
    -- Called 104
    -- SIP/104-08d2fc28 is ringing
    -- SIP/104-08d2fc28 answered SIP/101-b7b01f30
    -- Packet2Packet bridging SIP/101-b7b01f30 and SIP/104-08d2fc28
[Feb  4 20:59:28] NOTICE[4045]: rtp.c:788 process_rfc3389: Comfort noise support
 incomplete in Asterisk (RFC 3389). Please turn off on client if possible. Clien
t IP: 10.1.3.6

*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status

104/104                    10.1.3.6         D          5061     Unmonitored

103/103                    10.1.3.27        D          7994     Unmonitored

102/102                    10.1.3.12        D          41336    Unmonitored

101/101                    10.1.3.5         D          56702    Unmonitored

4 sip peers [Monitored: 0 online, 0 offline Unmonitored: 4 online, 0 offline]
*CLI>
```

Figure 3.4: Asterisk(PBX)console(Using client registration)

After configuration of Asterisk and x-lite,all calls and messages route via asterisk.so x-lite call connection and message information can observe on asterisk console.

Status on asterisk when clients call and message route though it shown in below:

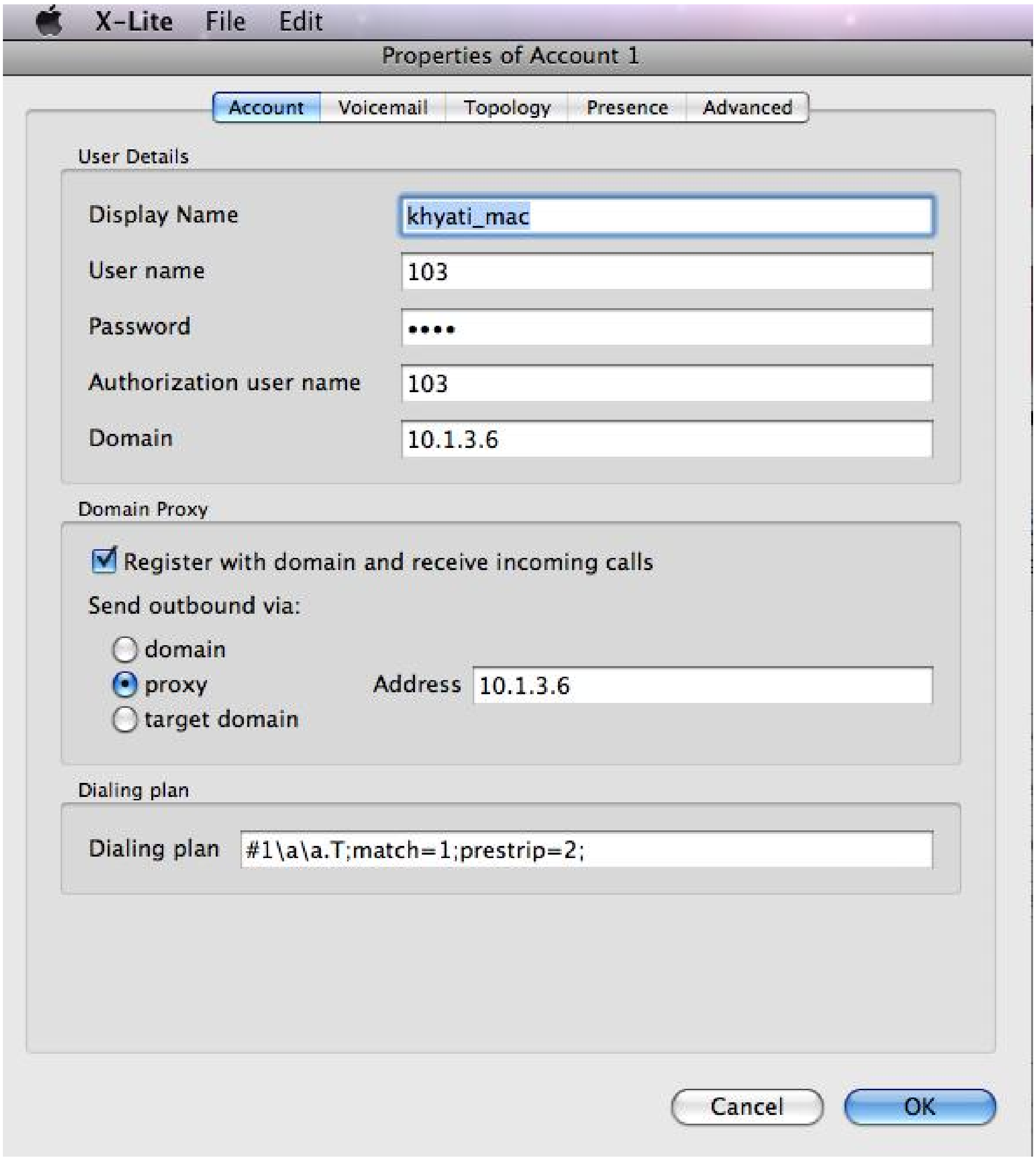

Asterisk Console on 'nirav' (pid 3908)
File Edit View Terminal Help

```
    -- SIP/101-08d2fc28 is ringing
    -- Executing [104@from-sip:1] Dial("SIP/103-b7b004e8", "SIP/104|20") in new
stack
    -- Called 104
    -- SIP/104-b7b0a8c8 is ringing
    -- SIP/104-b7b0a8c8 answered SIP/103-b7b004e8
    -- Packet2Packet bridging SIP/103-b7b004e8 and SIP/104-b7b0a8c8
  == Spawn extension (from-sip, 104, 1) exited non-zero on 'SIP/103-b7b004e8'
    -- Nobody picked up in 20000 ms
    -- Executing [101@from-sip:2] Hangup("SIP/103-b7b01f30", "") in new stack
  == Spawn extension (from-sip, 101, 2) exited non-zero on 'SIP/103-b7b01f30'
[Feb  4 21:01:56] WARNING[3926]: chan_sip.c:9765 receive_message: Received messa
ge to "NIRAV_LINUX"<sip:104@10.1.3.6> from "WINDOWS XP_NITIN"<sip:101@10.1.3.6>;
tag=683f9641, dropped it...
  Content-Type:text/plain
  Message: HI

[Feb  4 21:02:02] WARNING[3926]: chan_sip.c:9765 receive_message: Received messa
ge to "KHAYTI_MAC"<sip:103@10.1.3.6> from "WINDOWS XP_NITIN"<sip:101@10.1.3.6>;t
ag=7a77ef02, dropped it...
  Content-Type:text/plain
  Message: HI
```

Figure 3.5: Asterisk(PBX)console(clients call and massage route via asterisk)

X-lite

After the complete installation and configuration of Asterisk,SIP account setting also require in x-lite so it can communicate via asterisk with other x-lite or other registered softphone.Sip account settings as per sip.conf files for its connectivity with asterisk shown in Figure 3.6 and After the sip account setting of x-lite. Figure 3.7 shows the session establishment of two softphones 101(XP)and103(MAC)after configuration of X-lite and Asterisk.



User Details

Display Name khyati_mac

User name 103

Password ••••

Authorization user name 103

Domain 10.1.3.6

Domain Proxy

☑ Register with domain and receive incoming calls

Send outbound via:

○ domain

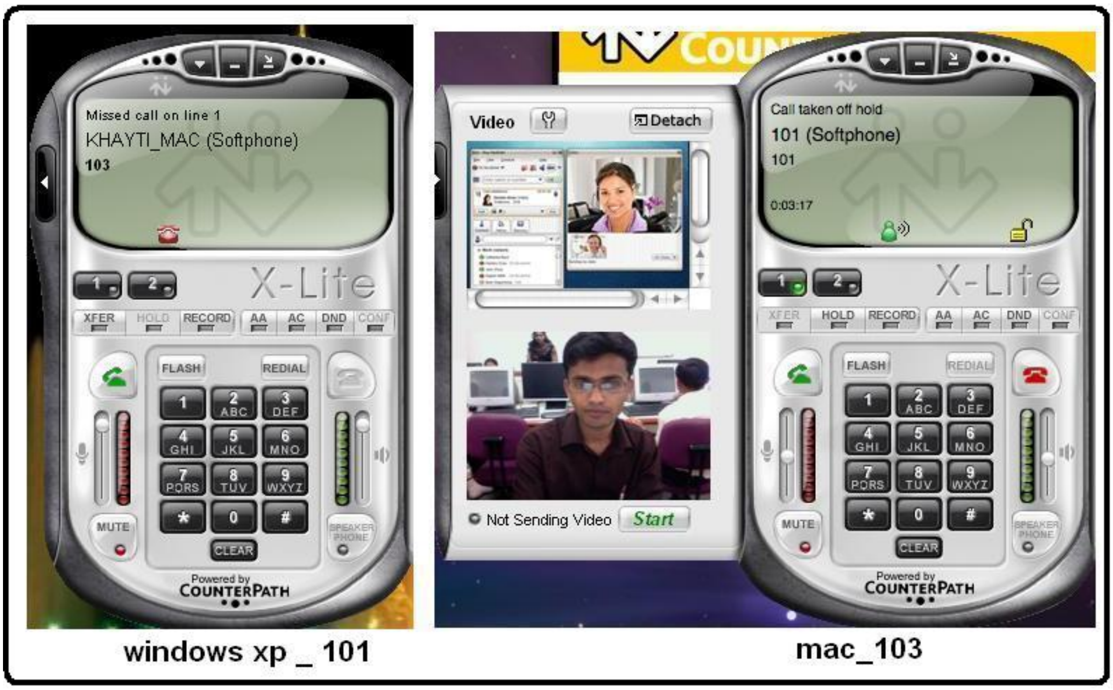
● proxy Address 10.1.3.6

○ target domain

Dialing plan

Dialing plan #1\a\a.T;match=1;prestrip=2;

Figure 3.6: X-lite Softphone(client registration)



Missed call on line 1
KHAYTI_MAC (Softphone)
103

Call taken off hold
101 (Softphone)
101
0:03:17

Not Sending Video

Figure 3.7: X-lite Softphone(client 101 connected with client 103)

Chapter 4

SPIT generation

This chapter describe the detail study and implementation of manually Spam(SIP invite traffic)generation which works as Spitter.

In order to implement the AntiSpam framework for a VOIP system,automatic VoIP Spam needs first.VOIP spam can be automatically generated and routed without the involvement and control of a proxy server or registrar.Without specific SIP configuration knowledge of the target phone,a fake INVITE message can send to the target and a SIP session can successfully establish to broadcast spam messages.This work can verify by the test result from simulation software SIPp and ngrep monitoring tool.

4.1 Feasibility of Manually VOIP Spamming

Implementation of an automatic VOIP generator works based on two different scenarios,depending on whether the Spam needs to go through the proxy servers in the VoIP system or not.Sending out the Spam messages through a proxy server is not an optimized idea for VoIP Spamming. If the spammer is a registered user of the PBX,a simple program can be implemented to just auto-dial a range of numbers and flood the VoIP Spam out through PBX.In this case,the big volume of voice mail coming from one registered user to pull up the attention of the proxy server.PBX can easily notice and detect the unusual communication behaviors with Spam detection methods.

In the other case,the attacker chooses to send out the Spam messages without going through the proxy server(or PBX), Spam detection schemes based on the server side will not be able to protect the SIP network any more. In the real world, the smart spammers tend not to route their voice spams through a specific proxy server. Since the spammer is an unregistered user and messages are not routed through the PBX, it has no control over the spamming situation. Compared to the previous case,it is much harder to detect. So the implementation of spammer machine based on these criteria is main challenge.

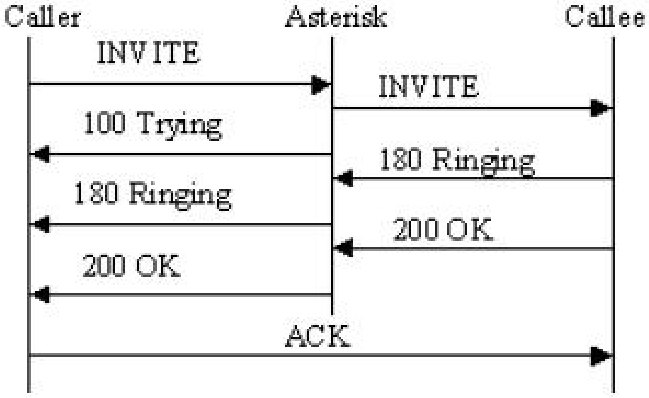


Figure 4.1: Signaling process of a regular SIP Call

METHOD-1

4.2 SIP invite flooding using sipp xml scenario and X-lite

Sipp is an open source SIP traffic generator tool and highly configurable to generate SPIT. Given the SIP service address (ID), Sipp generates SIP packet flow. It is use to flood VoIP network with large number of SPITs even with pre-recorded audio. Sipp works based on scenarios.

On the other hand Sipp can use as an end user client at the other end of communication with some specific scenarios. Sipp has a specific set of scenarios in built but as specified earlier so new scenarios generation is possible.This scenario describes the messages to be exchanged.A scenario generally specified by an XML file. These XML files are nothing but a configuration which reads the SIP messages and its sequence to generate SIP traffic.

4.2.1 Implementation of Automatic VOIP Spamming

Based on the above analysis,it appears to be possible to send a VOIP Spam to the target's SIP-based soft phone without going through PBX.

It is most likely and challenging that if the spammer is not a registered user of the PBX and the phone number of the target remains unknown,the attacker can still automatically send out the VOIP Spam by searching IP addresses with the knowledge of binding open SIP port.

In the negotiation of a regular SIP phone, X-lite as the UA responds to the basic INVITE message without any authentication challenge during the session initialization process. This indicates that it is possible to send the Spam message to the target client without going through PBX.

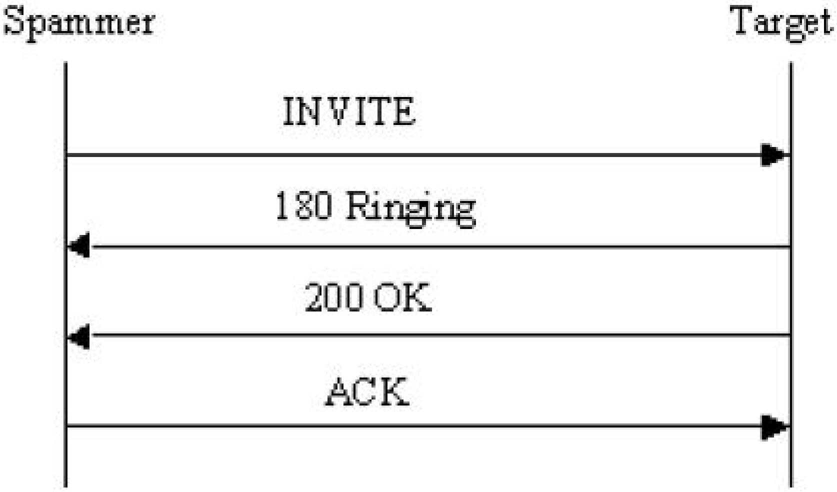


Figure 4.2: Signaling process of an automatically generated VOIP spam

4.2.2 Basic Format of INVITE message

Basic Format of INVITE message shown in below:

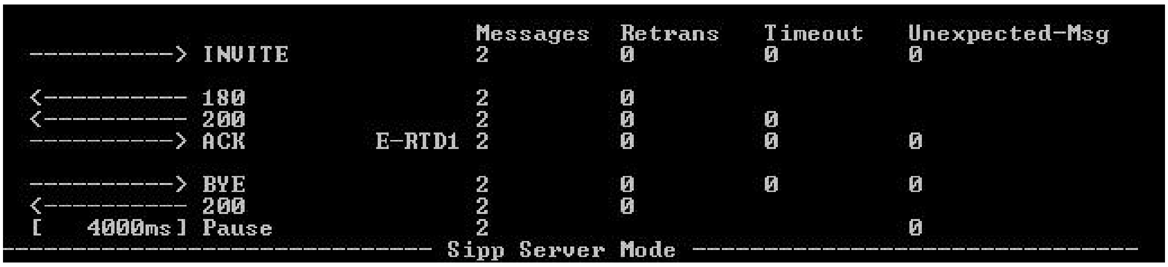
- INVITE sip <Target IP Address>
- Via:SIP/2.0/UDP <SPAmmer's IP address >
- Max-forwords:
- TO> Target IP Address <
- FROM <SPAmmer's IP address>
- Call_ID:

4.2.3 Sample XML Scenario for SPIT generation

- <scenario name="UAC with media">

- <send INVITE MESSAGE TEXT </send>
- <recv response </recv>
- <send> ACK MESSAGE TEXT </send>
- <nop> <action><SOME_PRERECORDED_MESSAGE"/></action> </nop>
- <pause milliseconds="8000"/>
- <send BYE MESSAGE TEXT </send>
- </scenario>

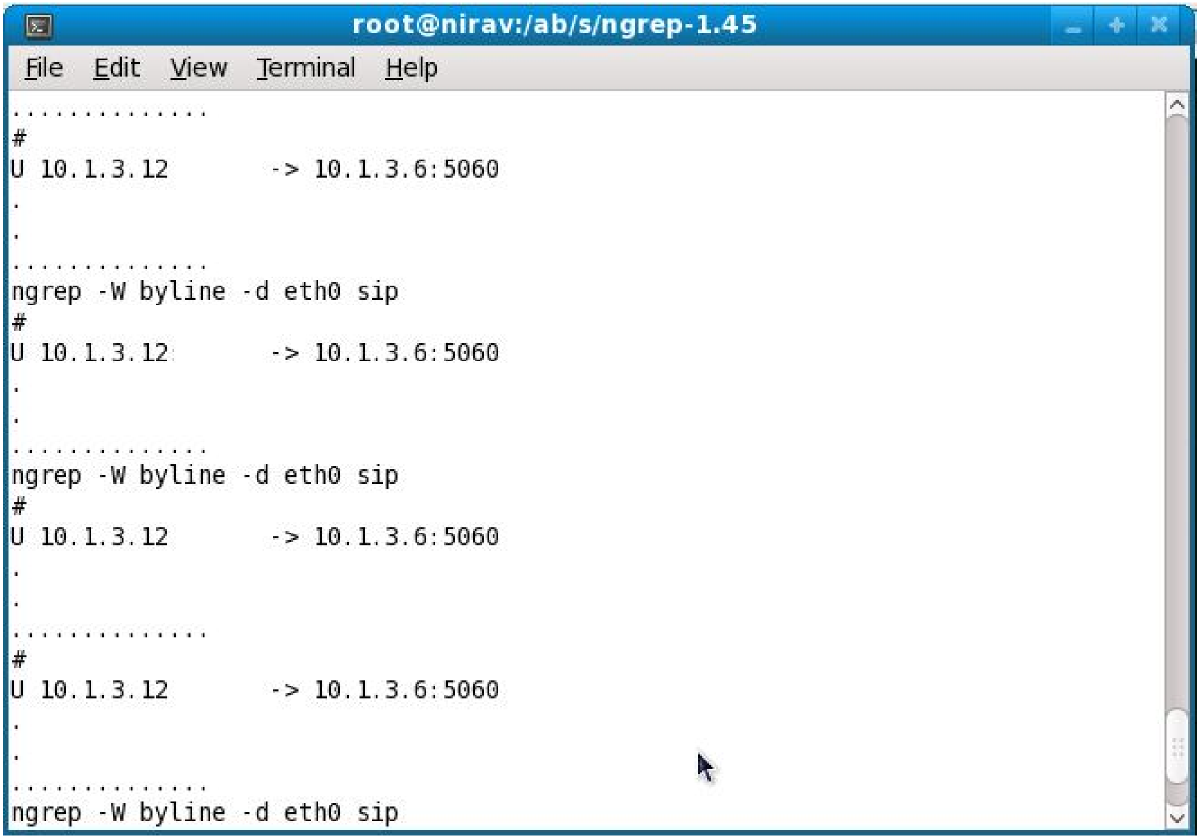
Using SIPp is an open source performance-testing tool,Manually generation of Spam phone calls(invite message)from SIPp UAC without registration with Asterisk and x-lite softphone sent the traffic to a registered X-lite shown in below figure 4.4.



```
                                 Messages  Retrans   Timeout   Unexpected-Msg
  ----------> INVITE             2         0         0         0

  <---------- 180                2         0
  <---------- 200                2         0         0
  ----------> ACK         E-RTD1 2         0         0         0

  ----------> BYE                2         0         0         0
  <---------- 200                2         0
  [   4000ms] Pause              2                             0
------------------------------ Sipp Server Mode -------------------------------
```

Figure 4.3: Results of SIPp after bulk spam call generation

Using Ngrep (linux based sip monitoring tool),Manually generation of Spam phone calls(invite message)monitoring shown in below figure 4.5.



```
..............
#
U 10.1.3.12       -> 10.1.3.6:5060
.
.
..............
ngrep -W byline -d eth0 sip
#
U 10.1.3.12       -> 10.1.3.6:5060
.
.
..............
ngrep -W byline -d eth0 sip
#
U 10.1.3.12       -> 10.1.3.6:5060
.
.
..............
#
U 10.1.3.12       -> 10.1.3.6:5060
.
.
..............
ngrep -W byline -d eth0 sip
```

Figure 4.4: Result of ngrep after bulk spam call generation

METHOD-2

4.3 SIP invite flooding using SIP invite flooding Tool

Inviteflood is used to generate a large number of INVITE messages, with spoofed source IP addresses. The attack can specify the range of IP addresses to be spoofed, as well as the spoofed username.

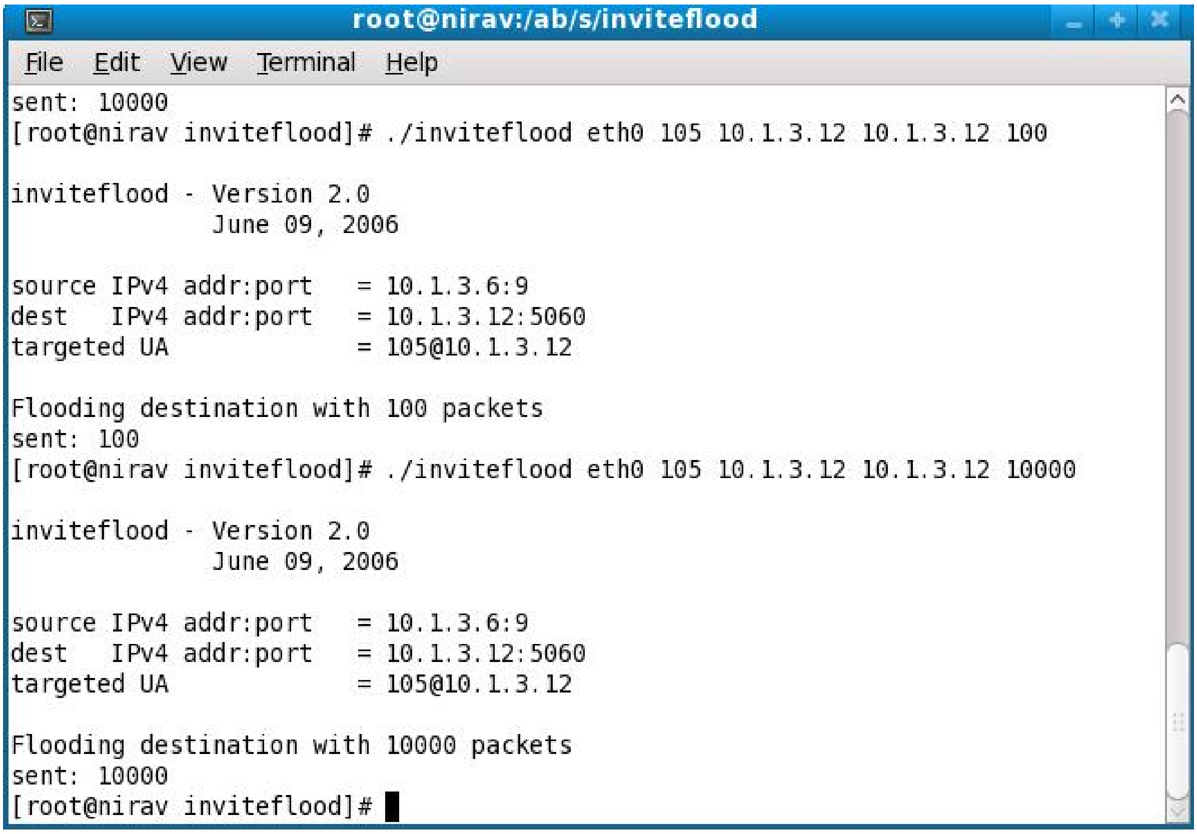
The inviteflood commands to send INVITE flood are:

```
./inviteflood eth0 UA-1 192.168.1.3 192.168.1.3 num_packets -s intervel
./inviteflood eth0 UA-1 192.168.1.3 192.168.1.3 num_calls -s intervel
```

where :

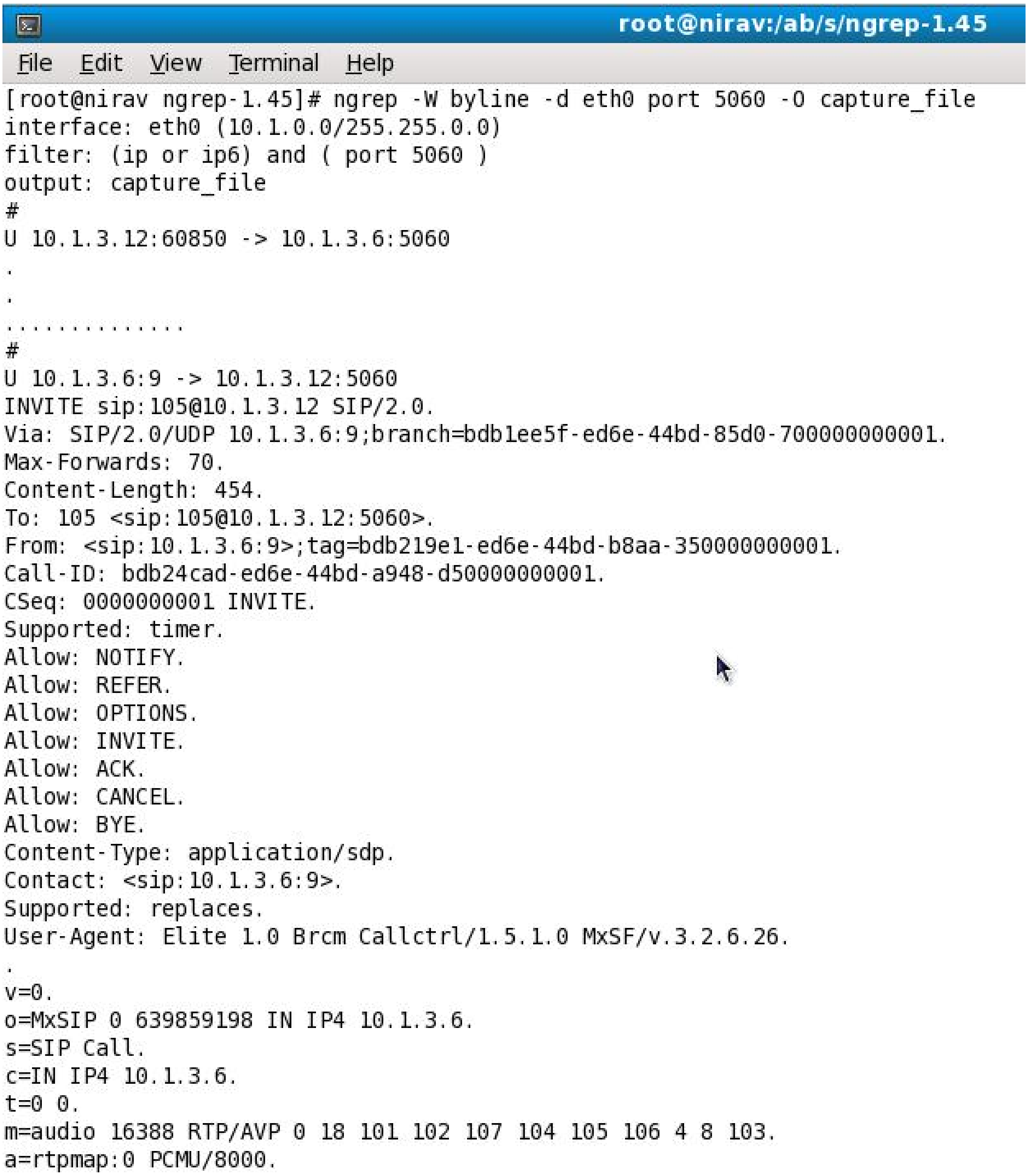
- eth0 is the network interface that the attack uses to send attack packets.
- UA-1 is the username of the target user
- 192.168.1.3 is the IP address of the target domain.
- 192.168.1.3 is also the IP address of the flood target.
- num_packets is the total number of attack packets to be sent.
- interval is the number seconds to wait between calls.

After configuration of invite flooding tool,SIP invite flooding can generate via above command and it can monitor using ngrep which is shown in below figure 4.6 and 4.7.From this experiment we can see that as the number of attack packets increases the call setup delay increases. When the amount of attack packets reaches a critical point, call setup will be timed out.This experiment demonstrates that a SIP-based VoIP system is vulnerable to SIP request flooding attacks which is shown in figure 4.8.



```
sent: 10000
[root@nirav inviteflood]# ./inviteflood eth0 105 10.1.3.12 10.1.3.12 100

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 10.1.3.6:9
dest   IPv4 addr:port   = 10.1.3.12:5060
targeted UA             = 105@10.1.3.12

Flooding destination with 100 packets
sent: 100
[root@nirav inviteflood]# ./inviteflood eth0 105 10.1.3.12 10.1.3.12 10000

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 10.1.3.6:9
dest   IPv4 addr:port   = 10.1.3.12:5060
targeted UA             = 105@10.1.3.12

Flooding destination with 10000 packets
sent: 10000
[root@nirav inviteflood]#
```

Figure 4.5: Console of SIP invite flooding tool



```
[root@nirav ngrep-1.45]# ngrep -W byline -d eth0 port 5060 -O capture_file
interface: eth0 (10.1.0.0/255.255.0.0)
filter: (ip or ip6) and ( port 5060 )
output: capture_file
#
U 10.1.3.12:60850 -> 10.1.3.6:5060
.
.
..............
#
U 10.1.3.6:9 -> 10.1.3.12:5060
INVITE sip:105@10.1.3.12 SIP/2.0.
Via: SIP/2.0/UDP 10.1.3.6:9;branch=bdb1ee5f-ed6e-44bd-85d0-700000000001.
Max-Forwards: 70.
Content-Length: 454.
To: 105 <sip:105@10.1.3.12:5060>.
From: <sip:10.1.3.6:9>;tag=bdb219e1-ed6e-44bd-b8aa-350000000001.
Call-ID: bdb24cad-ed6e-44bd-a948-d50000000001.
CSeq: 0000000001 INVITE.
Supported: timer.
Allow: NOTIFY.
Allow: REFER.
Allow: OPTIONS.
Allow: INVITE.
Allow: ACK.
Allow: CANCEL.
Allow: BYE.
Content-Type: application/sdp.
Contact: <sip:10.1.3.6:9>.
Supported: replaces.
User-Agent: Elite 1.0 Brcm Callctrl/1.5.1.0 MxSF/v.3.2.6.26.
.
v=0.
o=MxSIP 0 639859198 IN IP4 10.1.3.6.
s=SIP Call.
c=IN IP4 10.1.3.6.
t=0 0.
m=audio 16388 RTP/AVP 0 18 101 102 107 104 105 106 4 8 103.
a=rtpmap:0 PCMU/8000.
```

Figure 4.6: Result of ngrep after SIP invite flooding

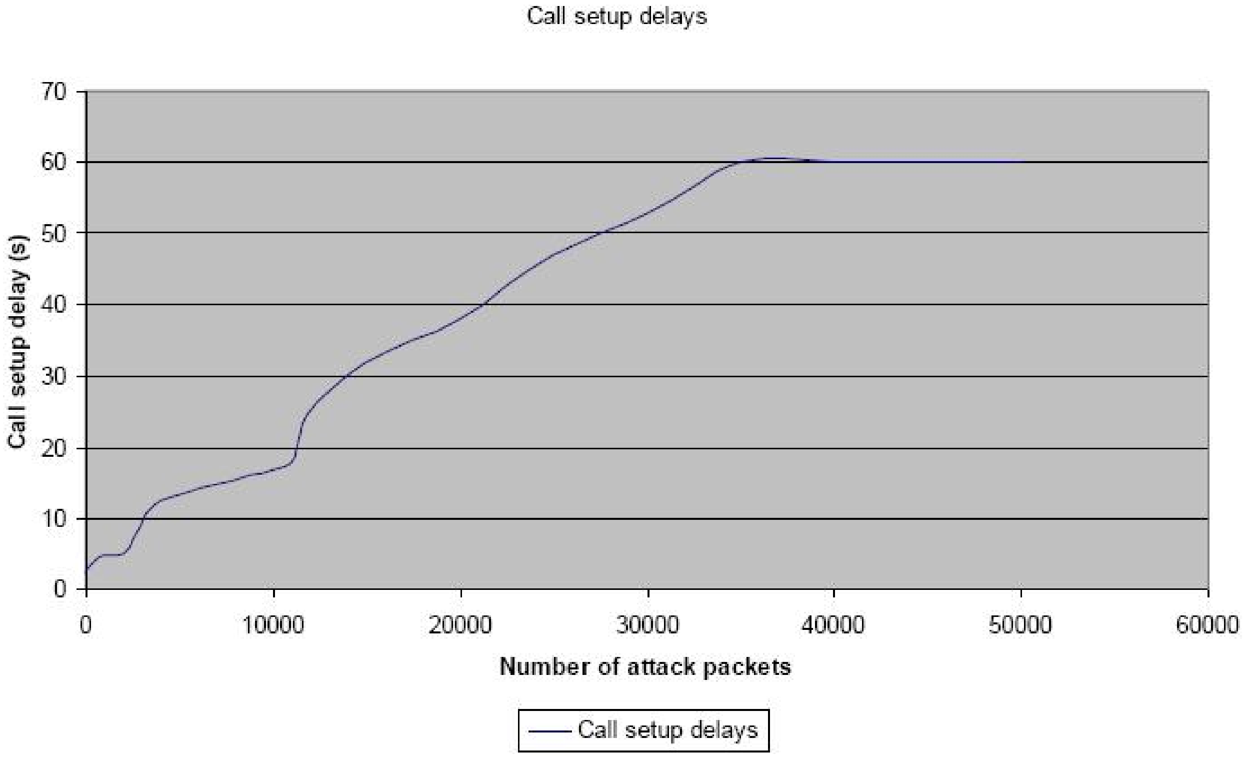


Figure 4.7: Call setup delay during SIP invite flooding

Chapter 5

Proposed Algorithm

This chapter describes proposed security-enhanced SIP system (SESS) consisting of a security enhanced SIP proxy server and an enhanced application layer stateless firewall.The basic concept of SESS is to maintain the firewall as well as the SIP server[9].

The enhanced SIP proxy server updates the firewall with the IP addresses of legitimate users and alerts the firewall when a legitimate user's IP address expire.An enhanced firewall adjusts its rules according to the information fed by the enhanced SIP proxy server and enforces advanced predictive nonce checking on unknown users. Additionally,a new protocol called Known Address Synchronization Protocol (KASP) is proposed to manage the update of legitimate user information between the security enhanced SIP proxy server and the reactive firewall.

5.1 Process of application-layer stateless firewall

Reduce the effect of the SIP flooding by initially proposed application-layer stateless firewall by improving predictive nonce checking mechanism.There is a unique field nonce in the SIP 401 (Unauthorized) and 407 (Authentication Required) messages to avoid SIP flooding attacks. A nonce is a server-specified data string which should be uniquely generated each time when 401 or 407 response is to be made[9].

The nonce is generated as a result of cryptographic function that is only known by the firewall.Since most servers have a timer to mitigate flooding attacks,the servers do not have to keep a record of the nonce.Thus, it is important for the firewall to improve performance using nonce checking.The firewall does not have to record the nonces with corresponding callIDs.But,when the re-request message arrives,the firewall can recalculate the nonce based on the received SIP header fields.If recalculated nonce match with the received nonce,the user is to be a legitimate user[9].

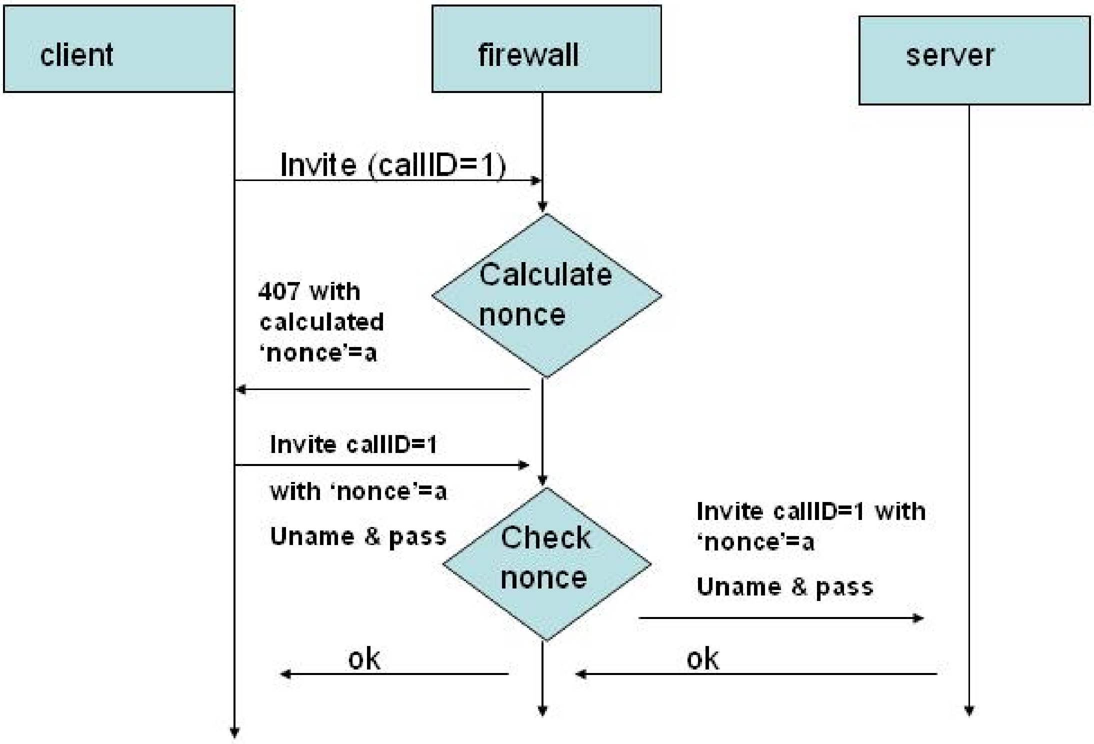


Figure 5.1: Call setup process with application-layer stateless firewall

Figure 5.1 shows the call setup process with firewall authentication using predictive nonce checking and Figure 5.2 illustrates,how the INVITE message is handled in detail:

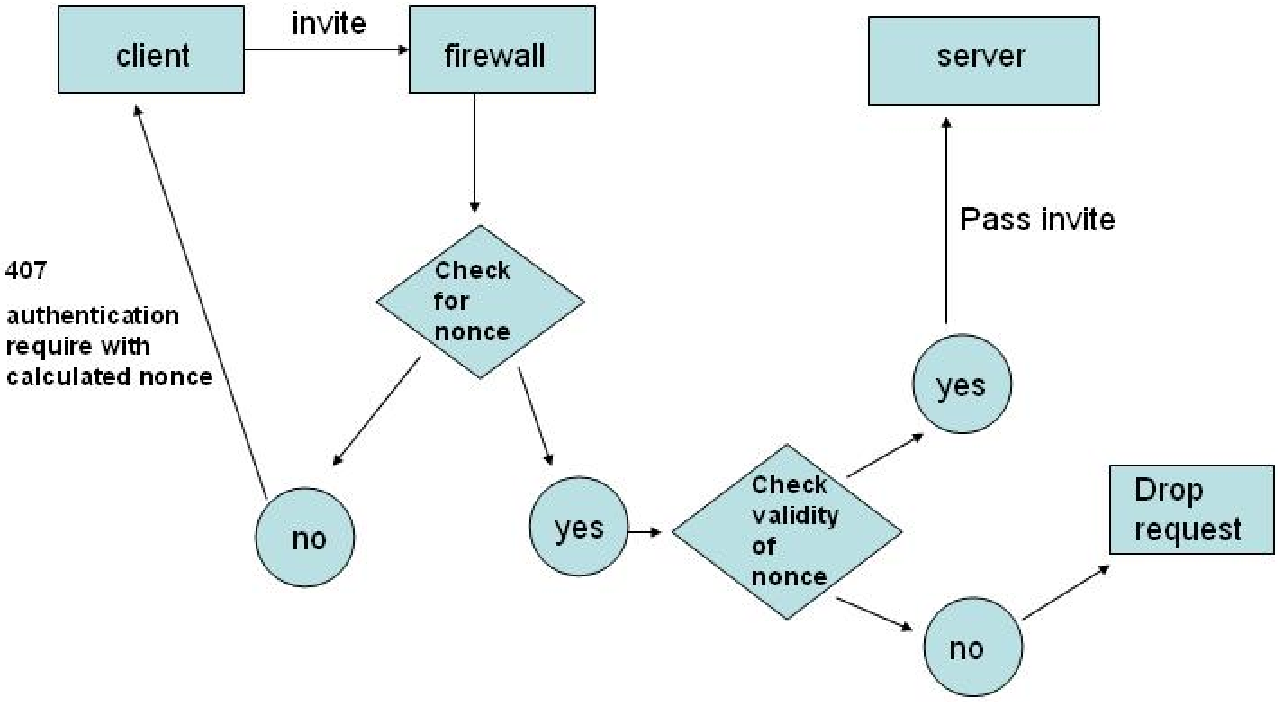


Figure 5.2: Process to handle an INVITE request

- When a message arrives at port 5060, the firewall checks if it is an INVITE or REGISTER message.If not,the message is allowed to pass through.

- If the message is INVITE/REGISTER, the firewall will check the SIP header, looking for a 'nonce' value.

- If the incoming SIP request does not have a nonce value, the firewall generates a nonce value which should be the result of a cryptographic secret function computed over the CallID and source IP address.This ensures that the nonce is unique for each session as a new CallID which is generated when a session is initiated.

- The firewall will send back a 407/401(Authentication Required/Unauthorized) message to the client with the calculated nonce value.Then the firewall will drop the session.

- After the client receives a 407/401 message,it resends an INVITE message with the same CallID,server-specified nonce,username and password.

- When the firewall receives an INVITE with a nonce value,it will recalculate a nonce value based on CallID and source IP address and compare it with the received nonce.

- If the nonce matches,the request is allowed to pass through to the server.

5.2 Process of Security-enhanced SIP proxy server

When a SIP request comes in at the firewall's SIP port(5060),it will check whether it is an INVITE or REGISTER.If it is, the firewall will authenticate the source by using improved predictive nonce checking.If not,it will just forward the request to the SIP proxy server.After the sender is authenticated,the re-INVITE and re-REGISTER will be passed to the SIP proxy server.

When the callee picks up the phone,a 200OK response is sent back to the caller via the proxy server.As soon as the caller receives the 200OK response, an ACK request is generated to inform the SIP proxy server and the callee about the success of the session setup.

When the SIP proxy server receives the ACK request, it knows the call setup three-way handshake is finished. At this point it has been established that the caller is a legitimate user. Thus, the SIP proxy server will extract the source IP address and record it in the legitimate user list. Following this, the SIP proxy server will update the firewall with the changes on the legitimate user list.

After the firewall receives the updates on the legitimate user list, it will convert those updates to iptables rules sets and issue them to the kernel iptables module.

5.3 Known address synchronization protocol(KASP)

KASP is used to transmit the updates of legitimate user lists from the SIP proxy server to the firewall using UDP. The reason to use UDP over TCP is that TCP is a connection oriented protocol which would need a three-way-handshake to establish a session before the data is transmitted. While TCP has better security than UDP, since the information update happens between a SIP proxy server and a firewall which is normally one hop away from the server, and given that the communication link is secured by the firewall, there is no real benefit to be gained from the security advantage of TCP. Additionally, as the update happens relatively frequently and the payload is small, it is very inefficient to go through the handshake process on each update.This protocol is also used to carry the legitimate user notifications.

5.4 Security-enhanced firewall

The security-enhanced firewall categorizes packets into three categories:frequent users, normal users and unknown users.Correspondingly, there are three queues on the firewall, namely: high-priority queue, normal queue and suspicious queue. Packets from hosts that are on the frequent user list will be put in the high-priority queue,if the packets are from a user list, they will be put into the normal queue. And if the source IP of the packets is not on the lists,they will be put into the suspicious queue. Packets in the high priority queue will have the highest priority, followed by the normal queue and they will be directly forwarded through the firewall to the server. Packets that are on the suspicious queue will be passed to the firewall's upper layer to be authenticated using the improved predictive nonce checking mechanism.

5.5 Implementation of SESS

5.5.1 Implementation platform

The enhanced SIP proxy server is implemented in Java using JAIN SLEE[9, 10].The reason for choosing JAIN SLEE is that it is designed for telecommunications low latency and high throughput environments.It also enables easy integration of new capabilities using a high level language Java. Jain SLEE is one of the most advanced network service environments available for network service development.

When implementing security-enhanced SIP proxy server,the SIP service component on JAIN SLEE server, called SIP Service Building Block is modified. Each incoming ACK message is logged and the IP address of the sender of this message is stored on one of the user list, depending on the time it made the last phone call. Hashtables are used to store the legitimate user IP addresses. There are two static hashtables created: frequentuserlist, and userlist.User source IP addresses are used as hashtable keys, and user objects are stored as hashtable values.

5.5.2 Java objects

The main Java objects created are as follows.

- A user object is created, which contains three attributes: a user source IP,a timer object,and a current time when the user request is handled.
- Timer objects are in charge of expiring the entry on its list. When the entry expires, the timer object will call a timer task object,which will perform a user removal action. If the user is removed from a frequentuserlist, it will be added to the userlist. If a user is removed from the userlist, the user will be considered to be unknown when they next make a phone call. The frequentuserlist has a shorter life cycle than the userlist. In the test environment, the frequentuserlist is set to expire after 10 minutes, and the userlist to expire after 15 minutes.

When a user completes the INVITE three-way handshake, the proxy server will carry out the enhanced security process as described previously.

5.5.3 Pseudo code of the userlist class

Pseudo code of the userlist class shown in below:

Pseudo code of the userlist class

```
if user is already on the frequentuserlist then
    Update timer;
end if
if user is on the userlist then
    if Timedifference < frequentuserlist expire time then
        Userlist.remove (user);
        Frequentuserlist.put(user);
        reset userTimer to frequentuserTimer;
        notify firewall about the change;
    end if
    Reset userTimer to userTimer;
end if
Userlist.put (user)
Notify firewall of the addition of user;
Set timer to userTimer;
```

5.5.4 Pseudo code of the remove user process

Pseudo code of the remove user process shown in below:

Pseudo code of the remove user process

```
REMOVE (user (userIP, which list it is on, timer)
if the user is in the frequentuserlist then
    Frequentuserlist.remove(userIP);
    Userlist.put(userIP, user);
    Notify firewall;
    if the user is in the userlist then
        Userlist.remove(userIP);
        Notify firewall;
    end if
end if
```

If the user is removed from the frequentuserlist,it will be added to the userlist, and a demotion notification will be sent to the firewall. If the user is removed from the userlist, notification of removal will be sent to the firewall.When the firewall receives a notification, it will map the notification to an iptables rule.

5.5.5 Implementation of the security enhanced firewall

The security enhanced firewall is implemented using a standard linux iptables firewall. Iptables rule sets are a true layer-three process with no application layer processing required, and this ensures optimal performance of the system.

The first requirement for the firewall is to enable destination network address translation (DNAT), and do regular SIP firewall setup. DNAT is used to prevent exposure of the SIP proxy private address.All requests that are received at the firewall's external interface on port 5060 will be forwarded to the SIP proxy. This is done by using the iptables DNAT rule set,eg:

```
iptables -t nat -A PREROUTING -p tcp -i eth0 -d 10.1.3.5 –dport 5060 -j DNAT
–to 10.1.3.6:5060
```

Then, the stateless SIP firewall is set up. After DNAT, all incoming SIP messages will be sent to the FORWARD chain. Thus, to ensure all SIP packets are passed to the stateless predictive nonce checking, we need to specify a firewall rule set as follows:

```
iptables A FORWARD p udp i eth0 d 10.1.3.6 -dport 5060 j queue
```

When an update packet is received,KASP message is to be converted into an iptables rule.

5.5.6 The advantages and drawbacks of the improved predictive nonce checking

The advantages and drawbacks of the improved predictive nonce checking are as follows:

- It can protect the server from Spoofed SIP INVITE and REGISTER flooding attacks.
- Stateless authentication : The firewall does not need to store multiple CallID and nonce entries in a database. This protects the firewall from RAM exhaustion during a flooding attack.
- There is a lack of kernel support as the predictive nonce checking is not native to the iptables firewall leading to slower than desired processing.
- It is based on an Iptables firewall, and uses IPQUEUE to pass each request from the network interface to the application layer. It is important to note that IPQUEUE contains a single FIFO queue to pass all relevant packets to the application layer. Thus, when this system is under flooding attack, it might slow down the call setup process for legitimate users as well.

5.5.7 The advantages and drawbacks of the SESS

The advantages and drawbacks of the SESS are as follows:

- Advantage : when the system is under severe INVITE or REGISTER flooding attack, the QoS of legitimate users is still maintained at a good level.
- Drawback : it can only block INVITE and REGISTER flooding attacks. It does not have a way to block other SIP request flooding.

Chapter 6

Test results and Analysis

This chapter covers experimental results of enhance AntiSPIT frameworks and detail analysis of test results based on the VOIP Quality of Service(QoS)parameters.

SIP invite flood is used to test the system performance.This is because SIP invite flood is considered to be a more harmful SIP attack traffic as it requires more processing power to process.The objective of this project is to find a solution which can stop the SIP flood traffic,mean while maintaining a good QoS for legitimate users.

6.1 VOIP QOS factors to verify proposed AntiSPIT solution

The following factors are measured to verify proposed AntiSPIT solution.

- Call setup delays when the system is under SIP flood attacks are measured.It's an important criterion to measure the QoS of a telephony system.
- Call setup timeout percentage is used to measure the availabilities of a system.
- CPU usages on the firewall and SIP proxy server when the system is under flood attack.It can help to improve the performance of the system.

Initially,the call setup delay is monitored when the system is operating with the firewall but without nonce checking.Then using the predictive nonce-checking firewall,the attack traffic managed through the firewall and the client call setup delay is be measured to verify the system performance.

Figure 6.1 illustrates the CPU usage diagram on the SIP proxy server when it using the application-layer stateless firewall.It shows that the application-layer stateless firewall is able to block all spoofed INVITE and REGISTER packets.

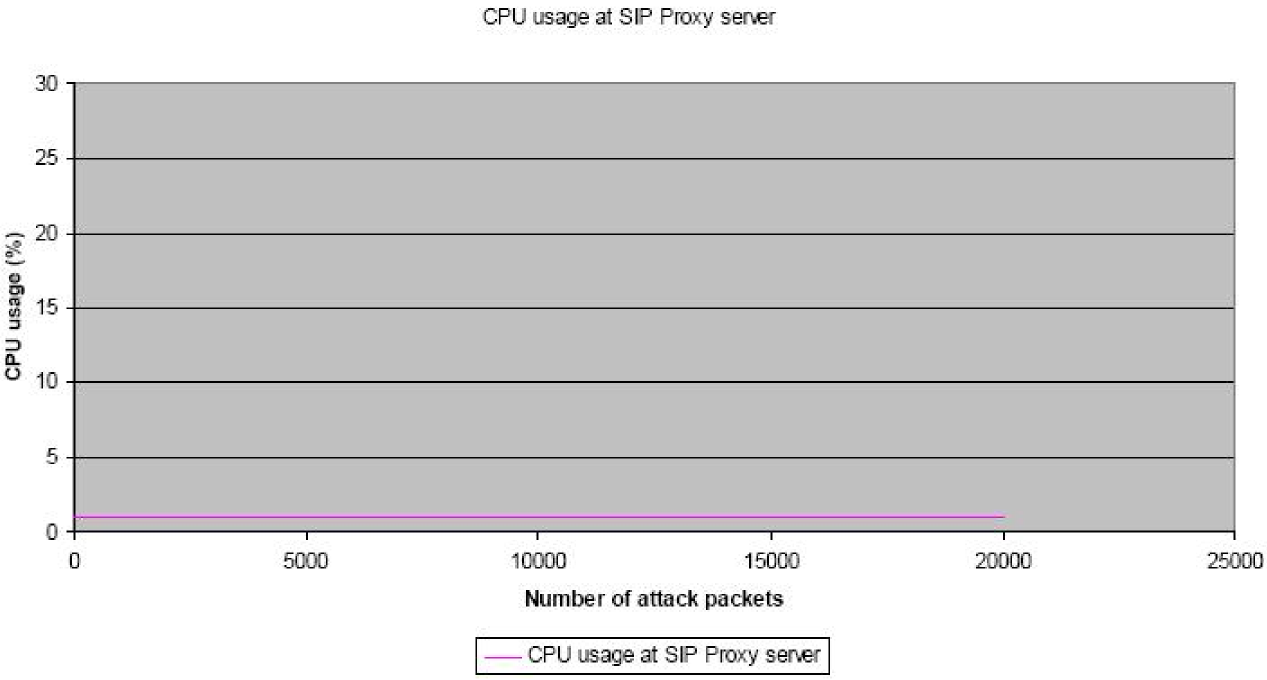


Figure 6.1: The CPU usage of the SIP proxy server during an INVITE flood attack

Figure 6.2 compares the call setup delays when the system is operating with the stateless firewall but without predictive nonce checking.The pink spikes in figure 6.2 represent call setup timeout.The application-layer stateless firewall helps to eliminates call setup timeouts.Call setup timeouts are caused by SIP proxy processing power exhaustion.There is no impact on the server and no call setup delays occur.

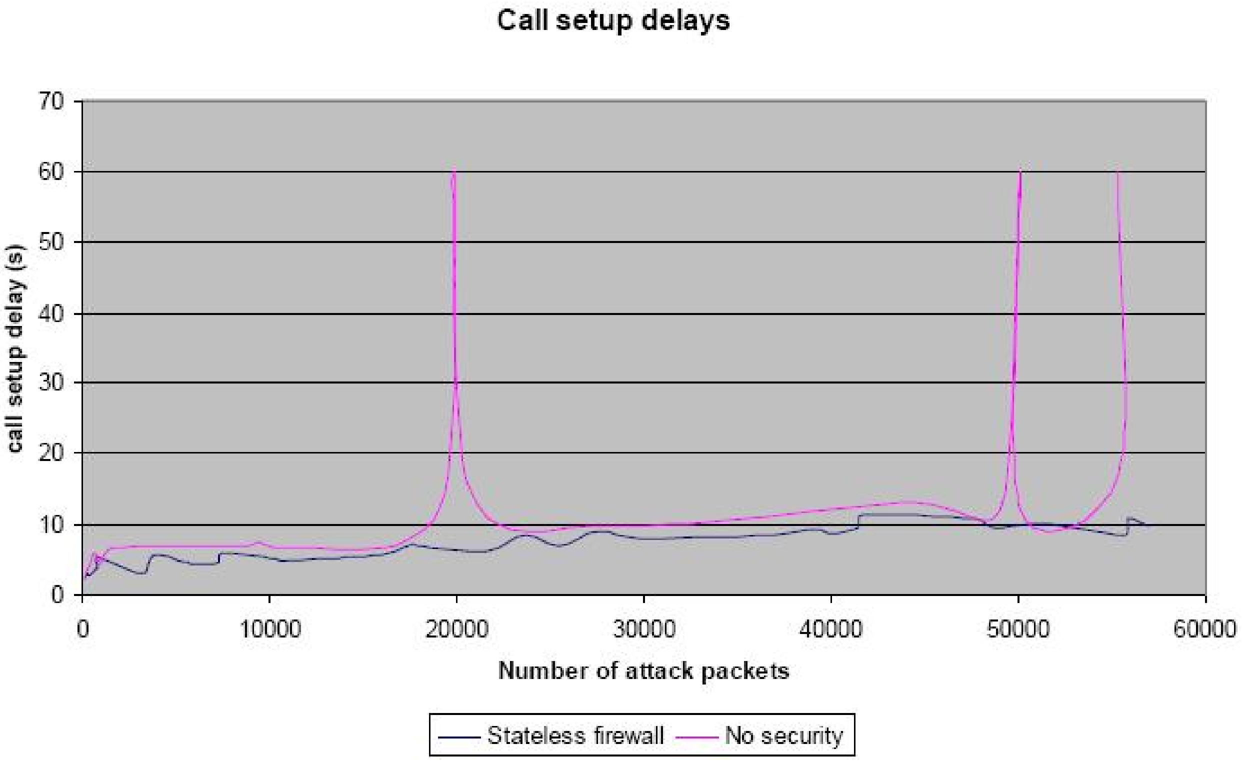


Figure 6.2: Comparison of call setup delays for stateless firewall and no security

From figure 6.2,the average call setup delay under an INVITE flood in an unsecured system is 9.39 seconds (call setup timeouts are not included in the calculation).Using the application-layer stateless firewall system,the average call setup delay is decreased by 25%(7.08 seconds)and this is mainly caused by the queuing and authentication process of the firewall.

While the use of application-layer stateless firewall can eliminate call setup timeouts and reduce the call setup delay by a quarter of that under no security,there is still a significant call setup delay.This confirms that the predictive nonce checking causes significant delays in the call setup process under flooding attack because of the predictive nonce checking is not native to a system so,there is no kernel support and a single FIFO queue is used to pass all SIP INVITE and REGISTER packets from the network interface to the application-layer process which makes the setup delay increase as per the number of attack packets increases.

In order to achieve good service performance for a legitimate user under a flooding attack,the proposed improved predictive nonce checking mechanism has to be used in conjunction with SESS.

6.2 CPU usages on the firewall and SESS

This experiment measures the CPU usages on both firewall and SIP proxy server during an INVITE flood when the system is under various security levels. Figure 6.3 illustrates the experimental results.

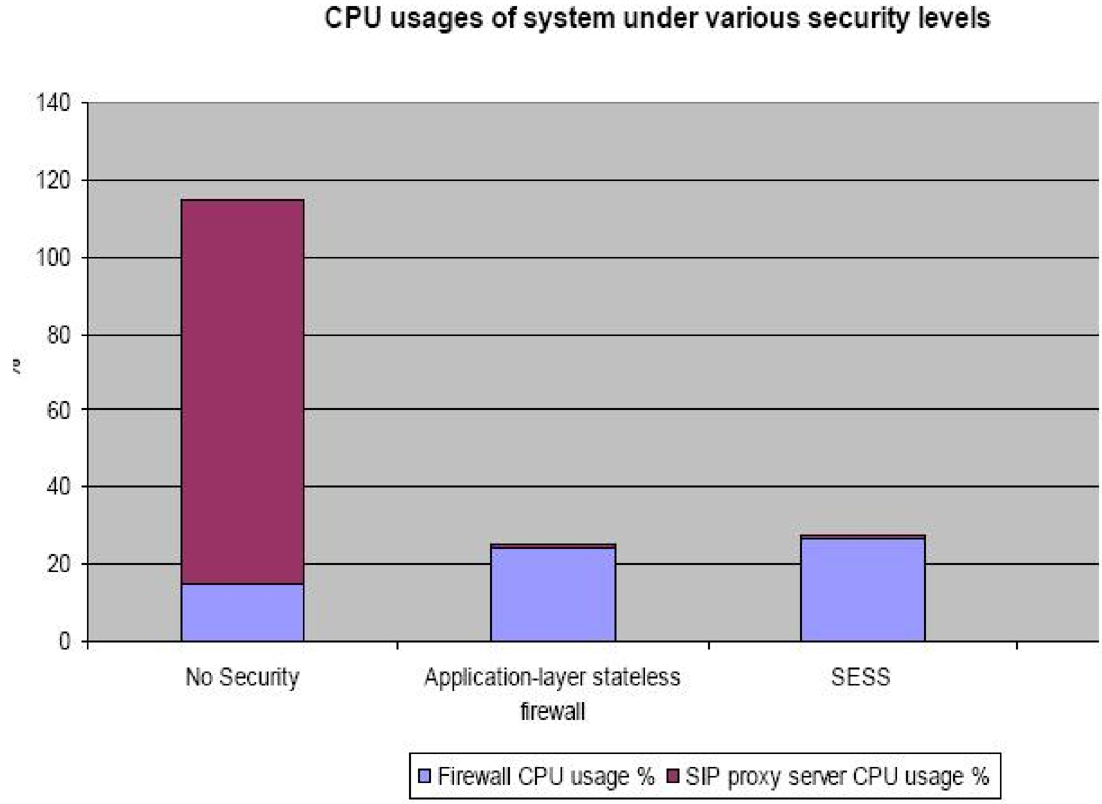


Figure 6.3: Comparison of CPU usages for firewall and SIP proxy server

As per above Figure 6.1,when there is no security deployed in the system the flooding attack can easily overload the SIP proxy server with spoofed requests (The server is almost at 100% CPU) and result in the high call setup timeout rate seen in the previous experiments. The average CPU usage at the firewall is only 15%, which indicates the firewall is not fully utilized.

When an application-layer stateless firewall is use, it will carry out much more processing than it does with its basic iptables forwarding(no security)rules.During the attack,the CPU usage on the firewall is only increased to 24%(9% increase)and it is still able to process other incoming requests.The CPU usage on the SIP proxy server is 1%.This is because only,legitimate requests are allowed to pass through the firewall.The SIP proxy server only processes a limited number of requests and the system is under an attack,the CPU usage on the proxy server should not be affected by the attack traffic.Thus,with authentication at the firewall,load balance is achieved and the SIP proxy server does not become overloaded by the attack.Further,there was no call setup timeout under the stateless application-layer predictive nonce checking system.When using SESS,the average CPU usage on the firewall increases to 26.5% due to spoofed requests being authenticated.

6.3 Call setup timeout percentages during flooding attacks

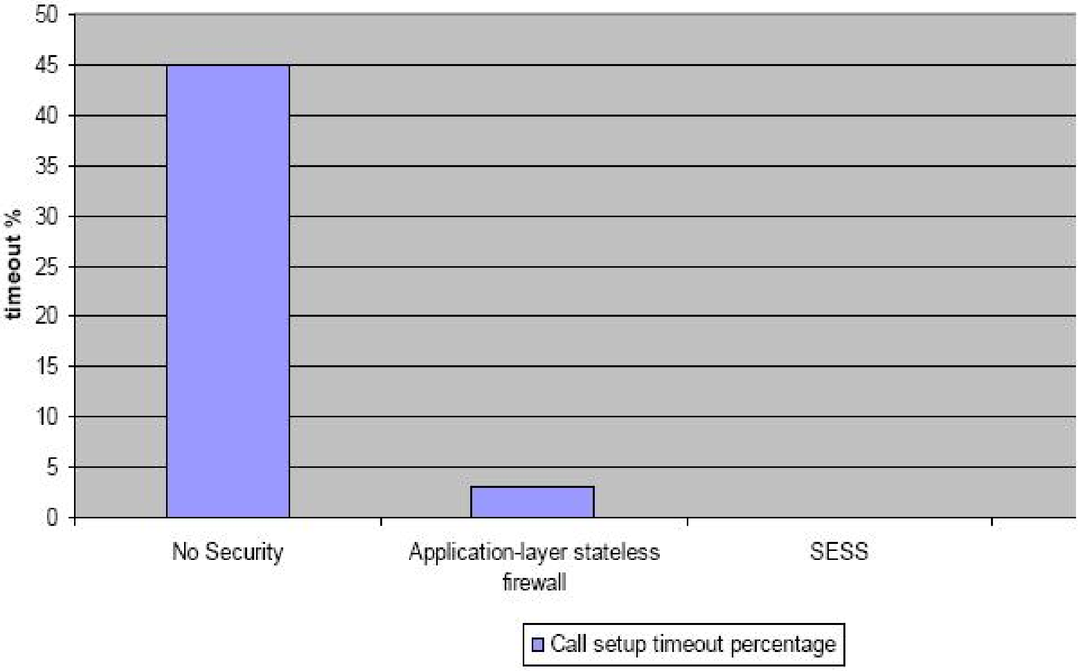


Figure 6.4: Average call setup timeouts under various security levels

As per above figure 6.4,the average call setup timeout during an INVITE flood,under no security is 14 times higher than that under application-layer stateless firewall.With SESS,there are no setup timeouts which improves the performance of this system significantly.

Chapter 7

Conclusion

Spitting describes the systematic scanning of a VOIP network with the target of gathering information about available user accounts,session establishment attempts as many users as possible in order to transfer any kind of message using SIP invite flooding.

In the stateless firewall scenario,all requests have to be authenticated with predictive nonce authentication and each request has to be processed twice which is very processing intensive and time consuming.So,the call setup delay is increased.There is only a single FIFO queue to pass the packets to the application layer,the time for packets waiting in the queue increases and when the system is under flooding attack the call setup delay for legitimate users will be increases.

By using SESS,known legitimate user's requests are passed to the SIP proxy directly,So its do not need to wait in the queue to be authenticated by the firewall.

SESS provides Good attack block success rate to block all SIP INVITE and REGISTER floods and high QoS for legitimate users when the system is under INVITE or REGISTER flooding attack.Main disadvantage of SESS is that,it can only block INVITE and REGISTER flooding attacks.It does not have a way to block other SIP request flooding like SIP ACK and SUBSCRIBE.So,SESS can be explore and improve to block SIP request flooding like SIP ACK and SUBSCRIBE.

Appendix A

Website References

1. http://www.ofta.gov.hk/en/ad-comm/tsac/cc-paper/ccs2005p11.htm

2. http://en.allexperts.com/e/l/li/list$_-$of$_-$sip$_-$software.htm

3. http://www.go2linux.org/linux-softphones-review-best-free

4. http://www.freshtechtips.com/2008/10/best-free-voip-softphone-applications.html

5. http://www.ip-pbx.co.za/blogs/asterisk-ippbx-benefits

6. http://sipx-wiki.calivia.com/index.php/Comparing$_-$sipXecs$_-$IP$_-$PBX$_-$with$_-$Asterisk

7. http://www.voip-news.com/faq/open-source-ip-pbx-faq/

8. http://www.asterisk.org/

9. http://sipp.sourceforge.net/

10. http://hackingvoipexposed.com/sec$_-$tools.html

11. http://ngrep.sourceforge.net/

References

[1] Ciaran O Donnell."SPIT: SPam over Internet Telephony",*School of Computing and Intelligent Systems University of Ulster,Magee Campus,Northern Ireland, BT48 7JL,UK*,2006

[2] G.F.Marias,S.Dritsas,M.Theoharidou,J.Mallios,D.Gritzalis."SIP Vulnerabilities and Anti-SPIT Mechanisms Assessment",*Information Security and Critical Infrastructure Protection Research Group Dept.of Informatics,Athens University of Economics and Business(AUEB),Greece*,2007.

[3] Yacine Rebahi,Dorgham Sisalem,Thomas Magedanz Fraunhofer Fokus,Kaiserin Augusta Allee."SIP Spam Detection",*Germany.*

[4] Juergen Quittek, Saverio Niccolini, Sandra Tartarelli,and Roman Schlegel."On Spam over Internet Telephony(SPIT)Prevention",*NEC Europe Ltd,*,2008.

[5] Jaesic Choi,Kangseok Chae,Jaeduck Choi,Souhwan Jung."Demonstration of Spam and Security Mechanism in SIP-based VoIP Services",*School of Electronic Engineering Soongsil University Seoul,Korea,*2009.

[6] Dr.Ghossoon M.Waleed Al-Saadoon."Asterisk Open Source to Implement Voice over Internet Protocol",*School Of Computer And Communication Engineering University,Malaysia,*2009.

[7] S.McGann,D.C.Sicker."An Analysis of Security Threats and Tools in SIP-Based VoIP Systems",*Proceedings of the 2 ndWorkshop on Securing Voice over IP, Cyber Security Alliance,*2005.

[8] H.Sengar,H.Wang,D.Wijesekera."Fast Detection of Denial of Service Attacks on IP Telephony",*Proceedings of the 14th IEEE International Workshop on Quality of Service(IWQoS 2006),*2006.

[9] Xianglin Deng,C.W.Lee."Security of VoIP-SIP flooding and its Mitigation",*New Zealand Computer Science Research Student Conference 08,*2008.

[10] S.B.Lim,D.Ferry"JAIN SLEE 1.0 Specification, final release", gg *Sun Microsystems, Inc. and Open Cloud Limited March,*2005.