VoIP Attacks & Security

By

Bhatia Ekta Ravikumar

12MCEI04

तमसो मा ज्योतिर्गमय

NIRMA UNIVERSITY

INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AHMEDABAD-382481

May 2014

VoIP Attacks & Security

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering
(Information and Network Security)

By

Bhatia Ekta Ravikumar

(12MCEI04)

Guided By

Prof. Dhaval Jha

NIRMA
UNIVERSITY
INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
AHMEDABAD-382481

May 2014

Undertaking for Originality of the Work

I, Bhatia Ekta Ravikumar, Roll. No.12MCEI04, give undertaking that the Major Project entitled “VoIP Attacks & Security” submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere, it will result in severe disciplinary action.

Signature of Student

Date:

Place: Endorsed by

Certificate

This is to certify that the Major Project entitled "VoIP Attacks & Security" submitted by Bhatia Ekta Ravikumar (12MCEI04), towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, 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.

Prof. Dhaval Jha
Internal Guide,
Department of C.S.E.,
Institute of Technology,
Nirma University, Ahmedabad.

Prof. Sharada Valiveti
Associate Professor, PGINS-Coordinator,
Department of C.S.E.,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
HOD [C.S.E. Dept.],
Institute of Technology,
Nirma University, Ahmedabad.

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

Mr. Shivdatt Patel
External Guide,
MIS & IT,
Colourtex Industries Limited, Surat.

Mr. Harshad Bardolia
Dy. General Manager,
MIS & IT,
Colourtex Industries Limited, Surat.

Abstract

VoIP Protocol is designed to carry voice data on the IP Protocol. Nowadays, apart from Voice there is a longing for data and video transfer also. This leads us to unified networks. In this thesis, All hardware-specific and network-centered attacks carried out in VoIP and their security issues will be covered alongside detailed countermeasures and hands-on implementation techniques. Initially the attacks will be conducted in order to understand the vulnerabilities and then I am going to research to find loopholes for how to defend against the latest Denial of Service attack, man-in-the-middle attack, call flooding attack, VoIP fuzzing, Voice SPAM/SPIT, and voice phishing attacks.

Acknowledgements

First of all, I would like to thank to the great power of **almighty god** that help me for each and every step of my life and guide me in true path to my vision. It is just about a day dream to work in **Colourtex Group** an esteemed organization especially on VoIP, my dream work area.

Then I would like to thank my **parents** and **friends** for their great support and suggestions. And I am also pleased to my college faculty members of **CSE department** including **Prof. Dhaval Jha** (my guide) and **Prof. Sharada Valiveti** (my PG Coordinator) for their excellent support during my academic time. I don't want to miss this opportunity to say "**Thank You**" for their magnificent efforts and support as friend and mentor.

I am also grateful to the awe-inspiring team of Colortex Group including **Mr. Harshad Bardolia**, **Mr. Shivdatt Patel** for giving me this golden opportunity and for expressing their confidence in me. I would like to express huge gratitude to **Mr. Girish Chaudhary**.

I want to convey my special thanks to

1. **R.K. Srivastava** Sir, Senior Scientific Officer Grade I at CFSL **C.B.I.** (Helping and Guiding)
2. **Sanjay Gautam** Sir, Coach at **The International Association of Computer Investigative Specialists** and Trainer at C.B.I. Ghaziabad Training Academy (Helping and Guiding me throughout)
3. **Goutam Roy** Sir, CFSL C.B.I. (Helping and Guiding)
4. **Vikas Sharma** Sir, CFSL C.B.I.
5. **Jetking** at Adajan, Surat (Lab & Technical support)

____

Signature of Student

Preface

Voice over Internet Protocol (Voice over IP, VoIP) is a general term used instead for of methodologies, transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks and communication protocols. The terms that are frequently encountered and often used along with VoIP are *IP* telephony, Internet telephony, broadband telephony, voice over broadband (VoBB), and broadband phone.

Goal:

To help people securely communicate with VoIP.

Vision:

"To enable the widespread and secure usage of VoIP possible which will be economic and cost effective way giving more features for communication"

Contents

List of Figures

Chapter 1

Project Profile

1.1 Project Profile

As we all know about VoIP which is the emerging technology in today's world substituting the old ways of communications. It's cheaper and provides more functionality as compared to them. It combines the data, voice and video together. But it is not having widespread usage due its vulnerabilities making it insecure for everyday usage. So here I am going to study about VoIP and it's working and not only studying but practically trying to implement those attacks too to create the same environment to conceptually understand what actually happens. Then this knowledge will help me to understand the vulnerabilities that are being exploited and then suggest some ways to overcome them making the communication more secure and VoIP more usable.

Chapter 2

Company Profile

2.1 Company Profile

2.1.1 Name

- Colourtex Industries Ltd.

2.1.2 Business Type

- Manufacturer / Exporter

2.1.3 Product/Service

- Dyestuff, Textile Dyes, Chemical

2.1.4 Corporate Address

- Survey No 91, Opp. Navin Fluorine Industries, Bhestan Road, Surat

2.1.5 Website

- www.colourtex.co.in

2.1.6 Listing Description

- Manufacturers of disperse dyes for polyester, reactive dyes for cotton etc.
- Shri Jayantibhai Jariwala, Chairman, Founded Colourtex in 1970
- ISO 14001:2004 & OHSAS 18001:2007 certified.
- ISO 9001-2008 certified.
- Commenced dyestuff manufacturing in the industrial suburb of Surat in 1976
- Today, with over 750 dyestuffs & chemicals from an installed capacity of 84,000 mt. in five manufacturing sites at Surat , Colourtex is the largest dyestuff producer in the country
- Unit 1 Coloursynth Industries
- 1983 Unit 2 Pandesara Dyes and Intermediates

- 1984 Unit 3 Vipan Industries
- 1991 Unit 4 Corachem
- 1997 Unit 5, Sachin
- 2007 all production sites merged in to Colourtex Industries Ltd

Chapter 3

Introduction

3.1 General

As we all know about VoIP which is the emerging technology in today's world substituting the old ways of communications. It's cheaper and provides more functionality as compared to them. It combines the data, voice and video together. But it is not having widespread usage due its vulnerabilities making it insecure for everyday usage. So here I am going to study about VoIP and it's working and not only studying but practically trying to implement those attacks too to create the same environment to conceptually understand what actually happens. Then this knowledge will help me to understand the vulnerabilities that are being exploited and then suggest some ways to overcome them making the communication more secure and VoIP more usable.

3.2 Motivation

- This (VoIP) technology has grown up very fast in the short past over the internet.
- The diagram on the right shows the increasing number of VoIP connections as compared to the decreasing number of PSTN (Public Switched Telephone Network) connections.
- A lot of security issues still need to be looked upon.

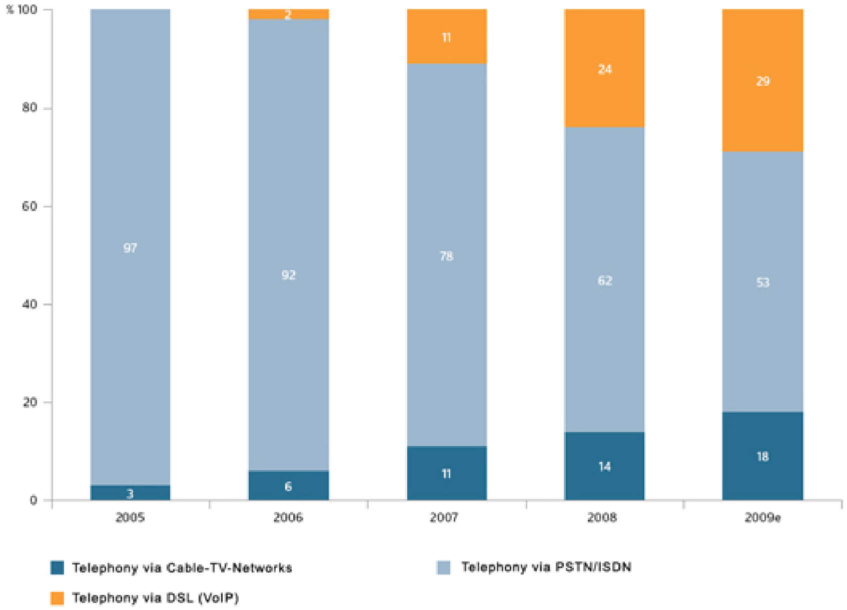


Figure 3.1: VoIP v/s PSTN.[2]

3.3 Objective

To find out vulnerabilities and loopholes in existing VoIP networks and try to eradicate or partially remove them making it more secure.

Chapter 4

Literature Survey

4.1 History

We, human beings always wanted to do something cool with our phones and computers.

In this thesis, I am going to explain that what is telephone and how it works? And also I am going to tell you about deal with data and voice in telephony technology. As we know that telephony is a big market today and being popular and common today. There are very few proper documentation available for telephony and I am trying to put my efforts to make it better for future generation.

First we are going to see the history of telephony.

4.2 Traditional Telephone Networks

4.2.1 PSTN

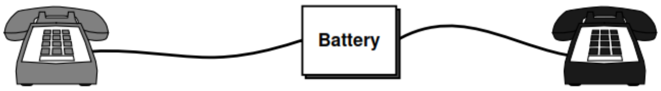


Figure 4.1: Simple Telephone Network.[3]

Here we see the simple network with two telephones and it was the first stage of communication and it was for defense department and it has limited usefulness.

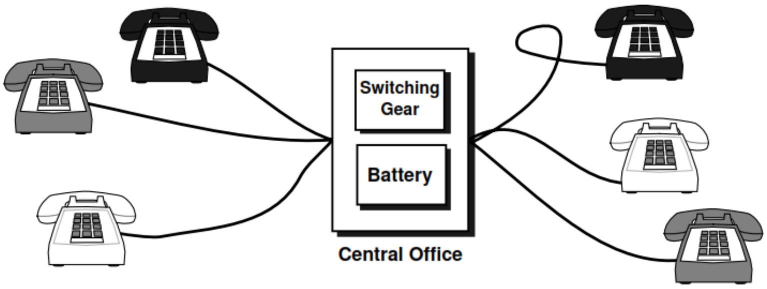


Figure 4.2: Local Network.[3]

Here we see more telephones connected to central office which provides necessary resources for communication such as voice battery, cables and etc. And you can call subscriber to central office or exchange.

It is also not so useful for calls out of the range.

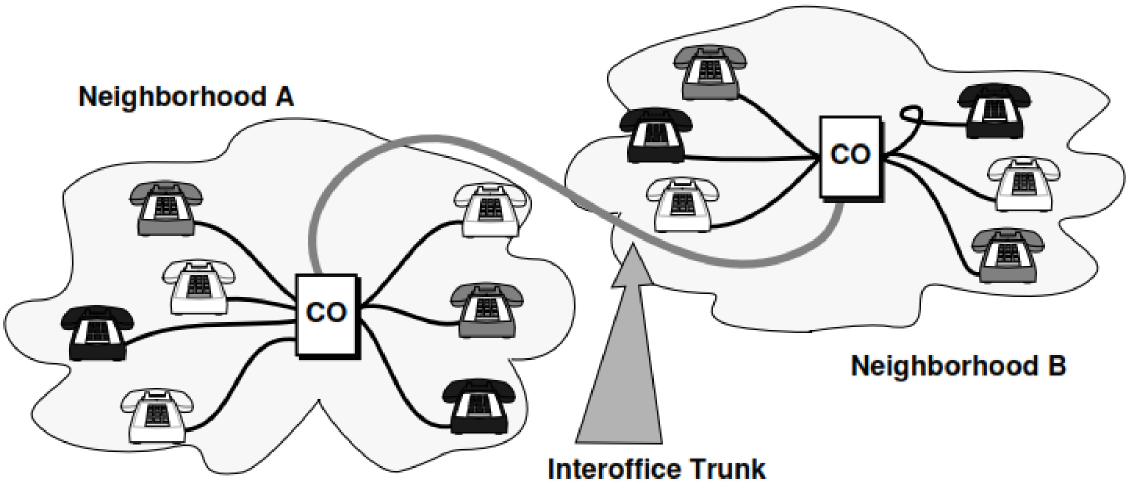


Figure 4.3: Interoffice Network.[3]

It is the internetwork between central office or exchange. Here the trunk is an ordinary phone lines and it has CO both sides.

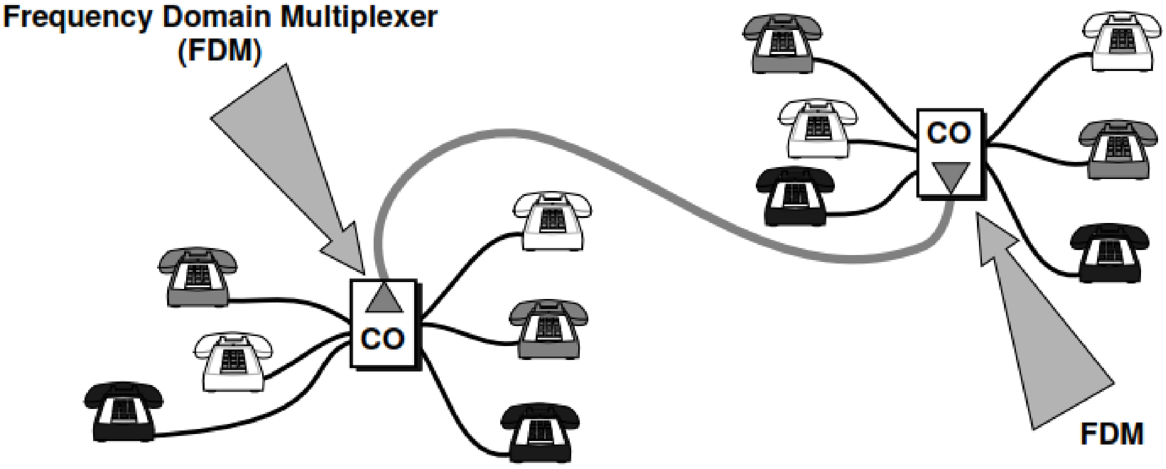


Figure 4.4: Interoffice Network using FDM.[3]

At the beginning of 20th Century, a cable once carried 24 voice signals. Signals are multiplexed in FDM on a single pair of wire and FDM divides 96kHz bandwidth into 24 uniform frequencies. It was available in the late 1800.

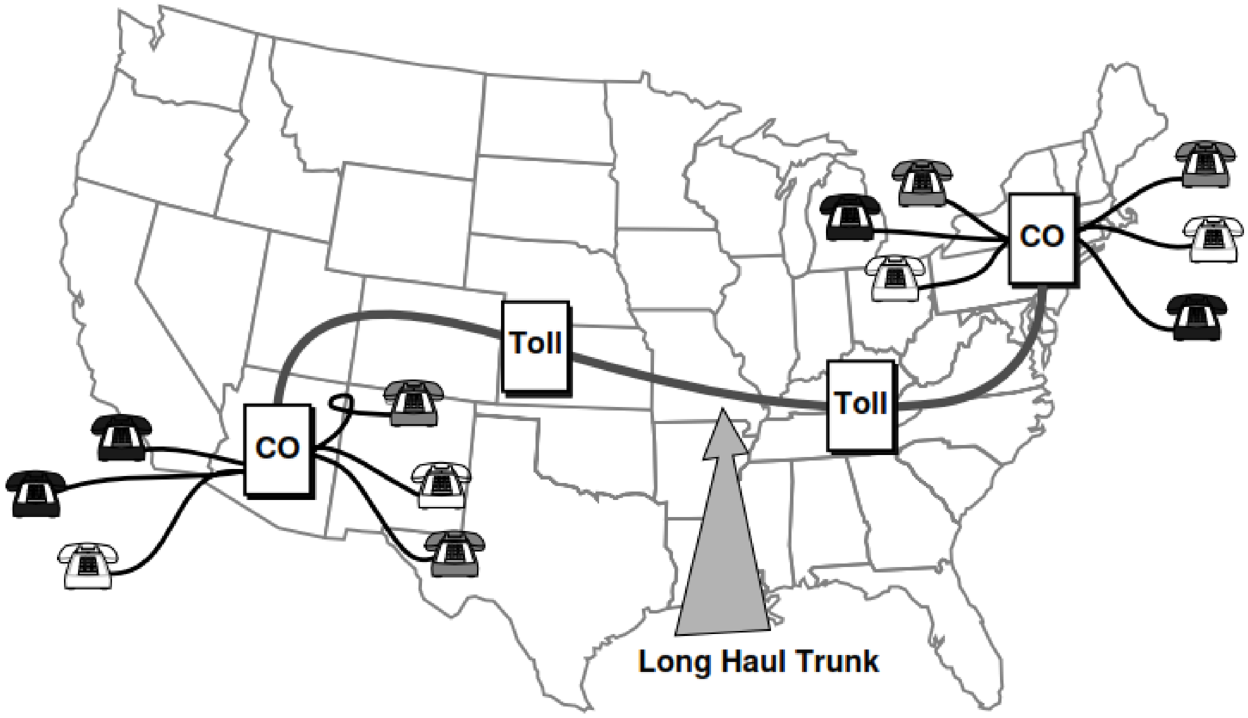


Figure 4.5: **Long Distance Connections**.[3]

So using FDM we can have 24 phone calls onto single trunk line but still long distance call problems were exists. And in long distance analog signal became weak and transmission facilities became very difficult. So T1 was developed to solve this problem over long distance.

4.2.2 ISDN[5]

It uses a circuit-switched techniques to allow video, audio and data transmission over existing phone lines. It is a low cost to Frame Relay or T1 and still able to provide high speed data connection than normal modem.

It provides two level services.

1. Basic Rate Interface (BRI): Use in small office or home connection.
2. Primary Rate Interface (PRI): For large enterprise or environment.

It also supports all protocols of network layer, operating systems and point-to-point protocol also.

ISDN Channels and ISDN Network

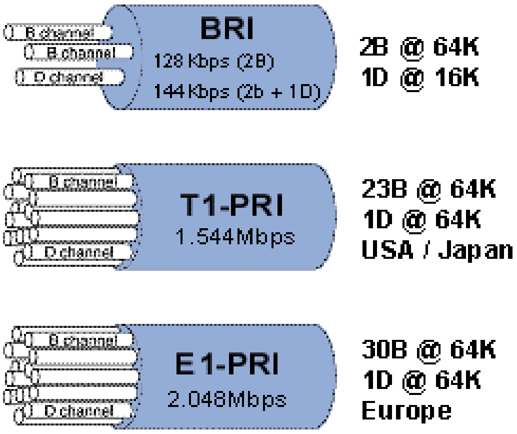


Figure 4.6: ISDN service.[5]

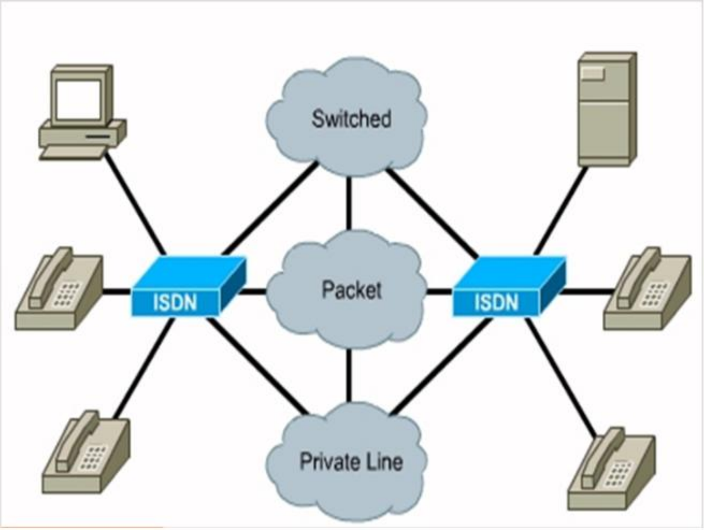


Figure 4.7: ISDN Working.

Some company providers offer ISDN connections with BRI. There three channels to provide this service.

1. At 16 kbps
2. At 64 kbps
3. At 128 kbps

And these channels are separated from data transmission channel.

Usage of ISDN:

- To add more bandwidth to communication
- To improve response time of the internet
- Support multiple network layer protocols
- Integration with other WAN services

4.3 Way of Unified Networks[6]

UCN is quite harder to implement than above technology.

- Through UC we can send voice mails to multiple phone numbers and faxes into mail boxes. And same we can do with email also.

- It is also used for instant messages, VoIP traffic solution and all the things you cans see using a single interface as INBOX.

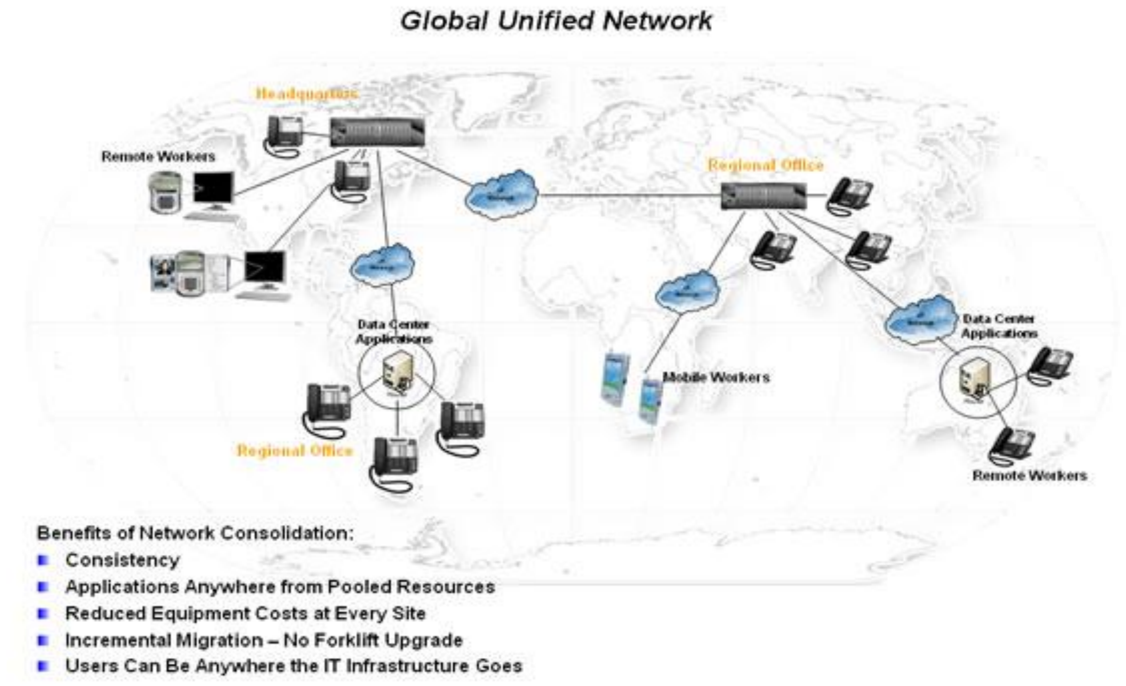

Global Unified Network
Headquarters
Remote Workers
Regional Office
Data Center Applications
Mobile Workers
Regional Office
Data Center Applications
Remote Workers
Benefits of Network Consolidation:
Consistency
Applications Anywhere from Pooled Resources
Reduced Equipment Costs at Every Site
Incremental Migration – No Forklift Upgrade
Users Can Be Anywhere the IT Infrastructure Goes

Figure 4.8: Global Unified Network.[6]

- UC is also used for web conferences and other real time communications.
- UC also can provide single email and using that single email use can transfer / send email, voice mails, instant mails, faxes and etc.

4.4 Unified Networks Needs[7]

- **For Business Continuity and Performance** – By best network communication will be flexible and effective.
- **Internet Access** – To deliver good internet base service faster way;
- **End-User Experience** – Very profitable to end-user experience in low budget.
- **Low Price** – In low cast we can get good and fast service;
- **IT management** – In management we can use to manage or establish new heights of quality of service to organizations.
- **Monitor** – We can monitor all the service to take a proper decisions.

Using Unified Network,

- **Guaranteed Performance** In average $300/user/month, we can provide better service to our thousands of clients.;
- **Efficiency:** It reduces workload provide faster networks globally.
- **Improve:** We can deploy application in speedy way;
- **Reduce Spending:** We can avoid bandwidth upgradation and save money.

4.5 Unified Networks' Future

4.5.1 RAN[8]

RAN is a new technology researching by the USA defence. And they are trying to relay VoIP services on radio signals called RAN.

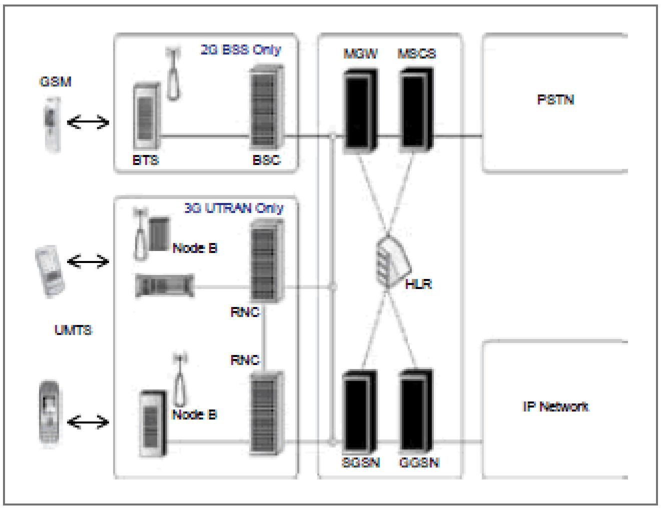


Figure 4.9: GSM/EDGE/UMTS

There two different RAN systems

1. GSM
2. UMTS

Using RAN we can use 2G, 3G, 4G networks in efficient way. And in RAN, it needs not to deploy separate RAN for different service. It means we can use multiple services in mix mode also such as UMTS, CDMA, TDMA and etc.

Figure 4.10 explains of SDR with both UMTS and GSM into a single RAN.

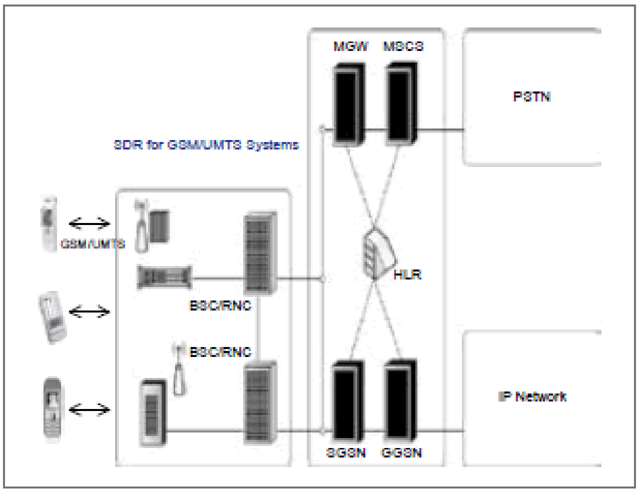


Figure 4.10: SDR-based UMTS/GSM[8]

There are many practical applications for example all GSM operators offer upgradation into new technology called UMTS without swapping anywhere. And it is compatible with existing technology.

RAN Architecture

1. Base Band Unit (BBU)
2. Remote Radio Unit (RRU)

It is to ensure extended coverage and with small size to give facility in easy way with great cost efficiency. It is also used to support green network concept.

- It provides a future proof network to the world.
- It gives more opportunity to mobile worlds

4.5.2 FoIP[9]

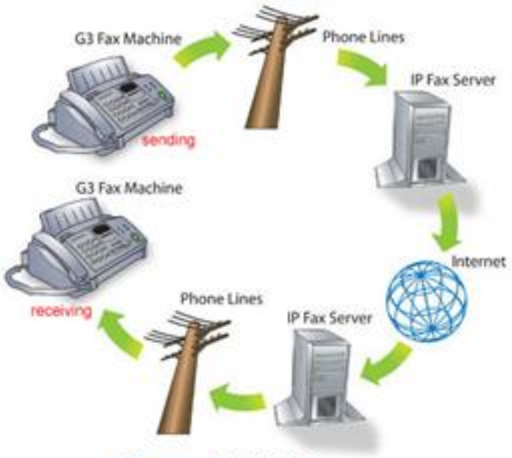


Figure 4-11 **FoIP**

Fax over Internet Protocol (FoIP), or IP faxing

- It is used to send fax from a computer.
- It is not used as regular fax session but instead of that beeps is being used when you are connected to destination machine.
- It gives nice and little confirmation for each successful transaction.
- It is cost saving
- It sends fax over Internet using VoIP
- You don’t need to buy a new FAX machine.
- You can use Fax machine by Internet.
- Transmission cost is very low.

Chapter 5

Technology Specifications

5.1 General Requirements

Internet network VoIP works with any type of Internet access such as..

- Dial-up
- Broadband DSL/ADSL and Cable Internet
- Dedicated lines (DS)
- Wi-FI and WiMax

Satellite Internet (not recommended due to latency issues)

5.2 Software/Hardware Requirements

- A software application also known as a Soft-Phone (Xlite and Zoiper used in Windows) is a dialer that we download on our computer or smart phone. Whenever we make computer based phone calls, we are running a VoIP soft-phone application, Skype for instance.
- By hardware we mean any VoIP hard phone equipment such as VoIP analog telephone adapter, VoIP Gateway, IP-Phone and many others types.

5.3 VoIP Service Provider Requirements

A VoIP provider, also known as Internet Phone Company or **ITSP** (Internet Telephony Service Provider) is a company that provides VoIP phone services and solutions similar to your local telecom companies. But they use VoIP technology to transmit our data, voice and video packets whereas traditional companies use PSTN lines.

VoIP providers offer different kind of VoIP services few to mention:

- VoIP home phone service
- VoIP for business
- VoIP solutions such as International calls through Call-shop, call back and calling card
- VoIP systems - conferencing, IP PBX, SIP Trunking, UC (Unified Communications)

Chapter 6

Attacks, Threats & Preventions

6.1 Current Scenario

6.1.1 Today VoIP Faces Problem

Because…

1. In compare of finding Software and Web based vulnerabilities, with telephony there is a lot of manual verification involved.
2. It is quite likely that a VoIP system that has a clear vulnerability will go unnoticed with current VoIP assessment tool.
3. It is also an area of industry where experience in multiple disciplines is generally required.
4. In order to understand a VoIP system there are a number of components to understand such data networks, unified networks, security background and voice technology.

6.1.2 Merging of VoIP

From a security point of view and even from a stability point of view merging is bad! Because…

1. It comes with added complexity in securing and data.
2. It shares many hardware and software components.
3. So many ways are there to attack.

6.1.3 Why is it Risky?

1. Working with VoIP with No different with working with mail routing, web access and databases.

6.1.4 General Solution

Simplest way to keep it separate from data components configures products appropriately, document and assess regularly.

6.2 Attacks

It is the research on well-known VoIP attacks which are basically focuses on the attacks that are associated with the SIP (Session Initiation Protocol).

1. Ability to hijack a legitimate user's VoIP Subscription & its subsequent communications
2. Ability to eavesdrop in to VoIP communications

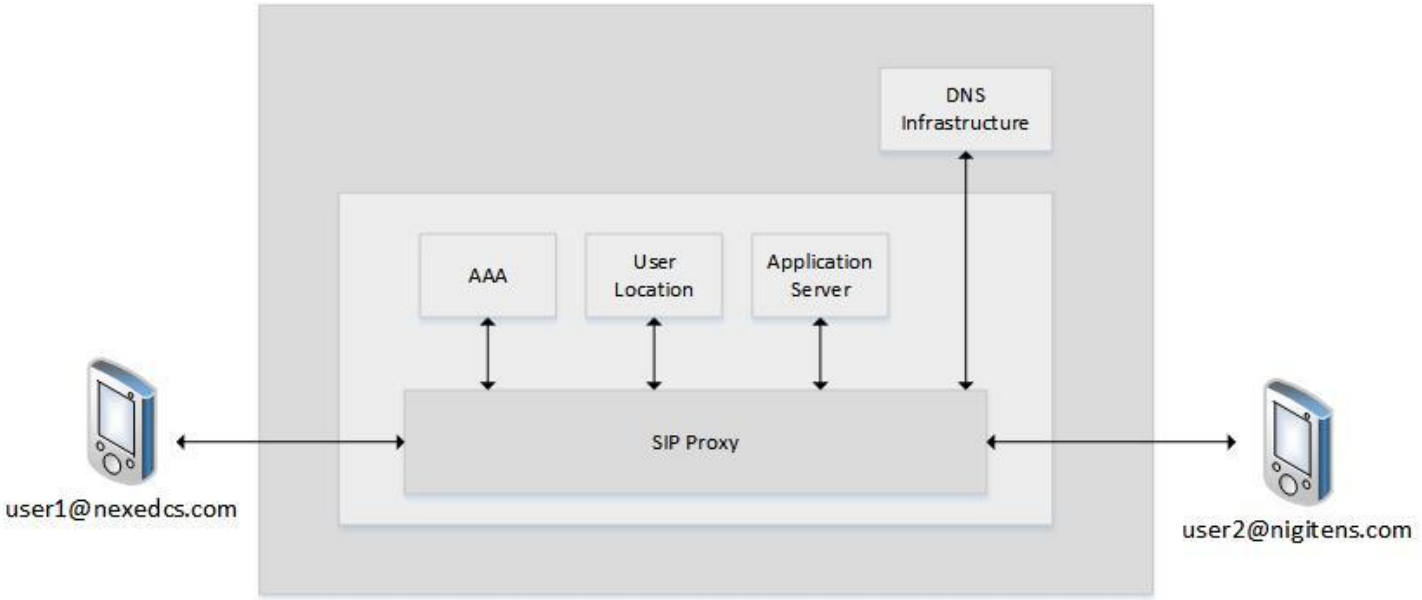


Figure 6.1: Current scenario of communication with SIP.

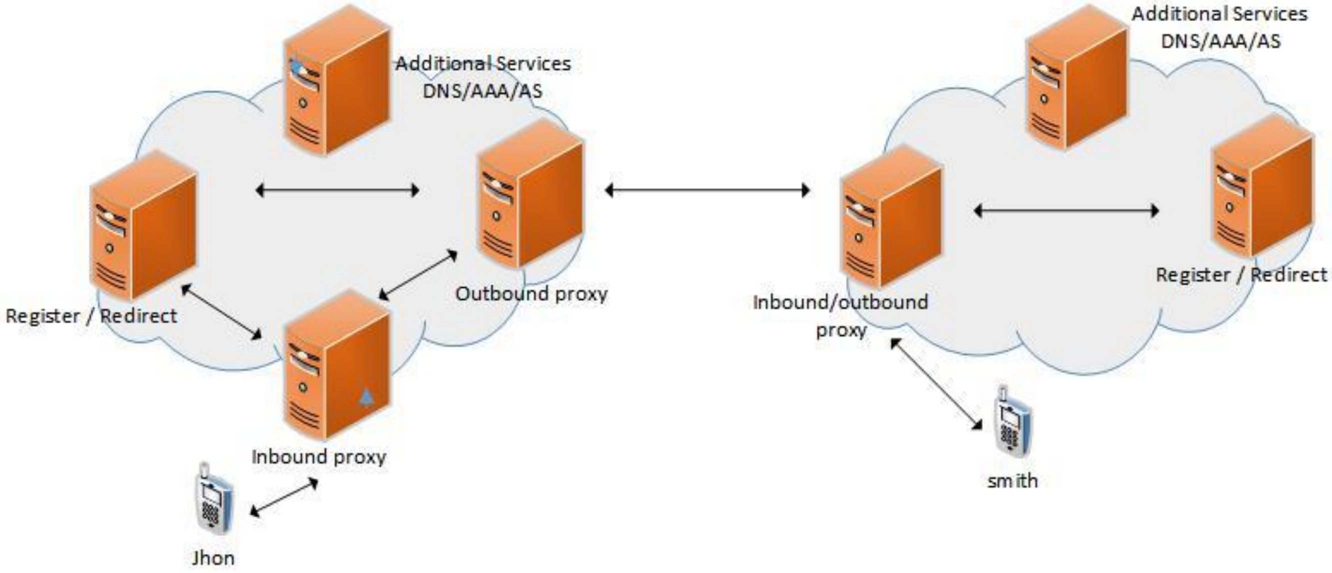


Figure 6.2: SIP Architecture in detail.

1. SIP has two type of states
   a. Transaction State: It is for receiving a request and ending it.
   b. Session state: In some cases we need session state for lifetime of a network such as NAT traversal in case of 3GPP (3rd Generation Partnership Program).
2. CPU: after we recieve the SIP messages, the SIP server need to parse message to do authentication, mapping to server, and forwarding.
3. Bandwidth: By loading the server's access link, anyone could easily cause the loss of SIP messages. It is transport-layer issue.

Industry experts have believed that these attacks are likely to become more apparent with the wider adoption of VoIP.

6.2.1 Attack 1: Registration Hijacking

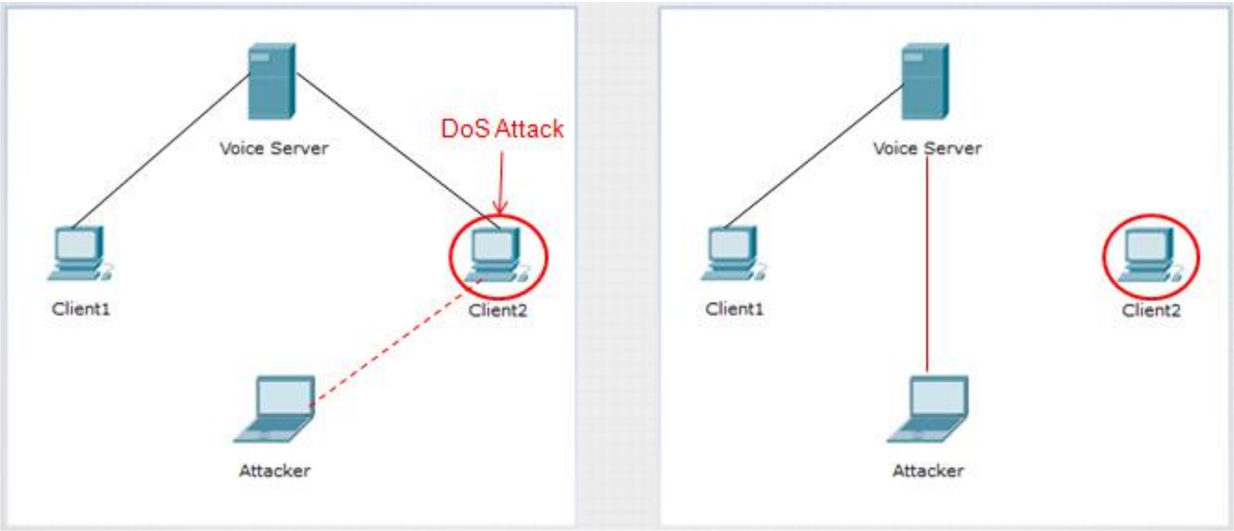


Figure 6.3: Network I used for Registration Hijacking.

1. In this attack, an attacker knows the addresses' structure.
2. An attacker can search registered addresses and using SIP INVITE or OPTIONS requests have been created using scanner.

For above both process, authentication may be required. And it is use by the proxy to identify the user or device.

Registration Hijacking Process

- It begins with an attacker who send a REGISTER request to a target machine to free all existing registrations. "Contact" header with (*) and "Expires" header with "0". Together it removes all registrations for the victim in the "To" line.
- An attacker send REGISTER request without Contact header lines. It tells to server to inform all registered contacts.
- An attacker can registered UA again on existing user.
- If a server asks authentication details with MD5 then an attacker tries to calculate MD5.
- After deletion of all contacts, an attacker sends again a REGISTER request with new Contact header.

Flow of Registration Hijacking:

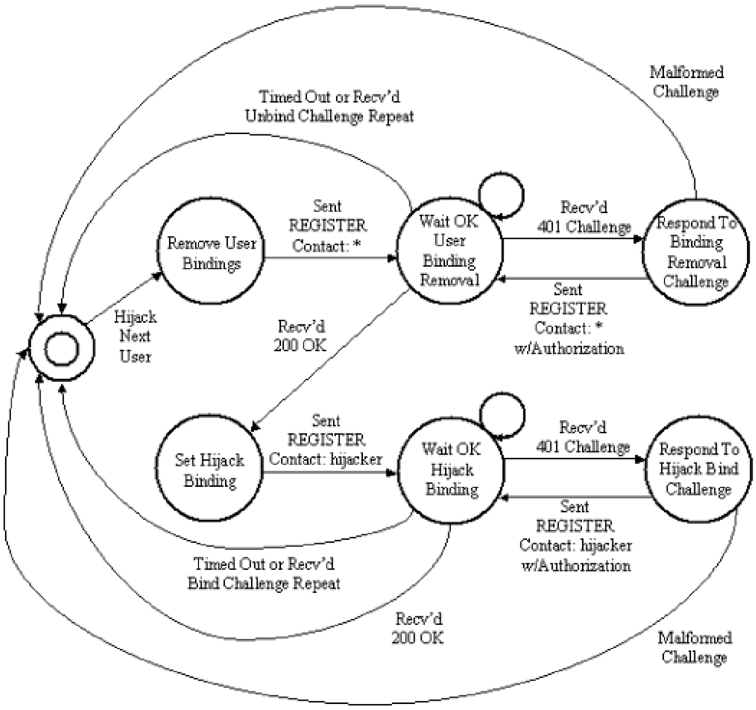

Timed Out or Recv'd Unbind Challenge Repeat
Malformed Challenge
Remove User Bindings
Sent REGISTER Contact: *
Wait OK User Binding Removal
Recv'd 401 Challenge
Respond To Binding Removal Challenge
Sent REGISTER Contact: * w/Authorization
Hijack Next User
Recv'd 200 OK
Set Hijack Binding
Sent REGISTER Contact: hijacker
Wait OK Hijack Binding
Recv'd 401 Challenge
Respond To Hijack Bind Challenge
Sent REGISTER Contact: hijacker w/Authorization
Timed Out or Recv'd Bind Challenge Repeat
Recv'd 200 OK
Malformed Challenge

Figure 6.4: Registration Hijacking Process Flow.

It is also performed by valid UA registered user. This attack is possible.

Prevention for Directory based attack

1. Need strong authentication.
2. Need to implement firewall to detect and block attack.
3. MD5 based authentication must be implemented.
4. Strong password must be selected.

Above steps are necessary to prevent directory based attack.

Prevention for External Network

1. UA must be implemented.
2. Detection while scanning of user directory.
3. Manage log report.
4. Identify unusual pattern of request.
5. Identify valid user using proxy server.
6. Define limit of REGISTER requests.
7. Network flow should be administrated.
8. Analyze failed attempts to identify guess passwords.

6.2.2 Attack 2: Eavesdropping

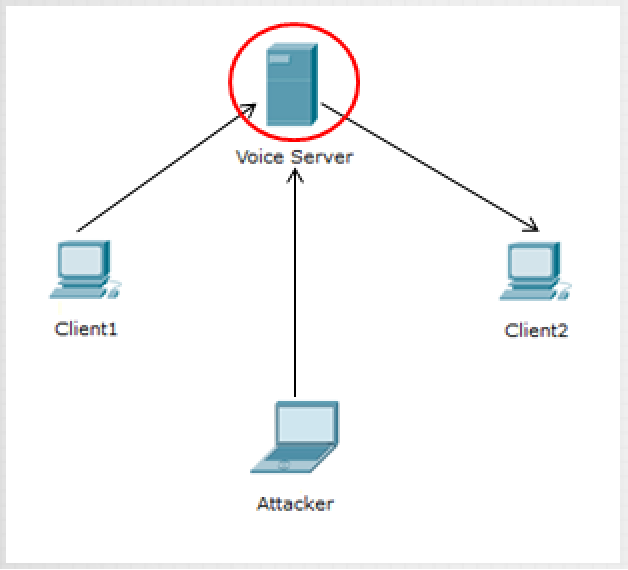


Figure 6.5: Network I used for Eavesdropping.

The signaling message use separate ports & network protocols (i.e., UDP or TCP) from the media itself. Media streams usually are carried over UDP Protocol using the RTP (Real Time Protocol). And Eavesdropping is used to capture that packets and convert into appropriate media format.

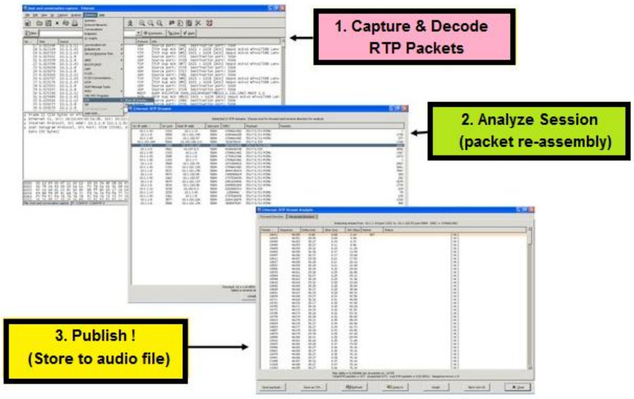


Figure 6.6: Steps to capture VoIP media streams using Ethereal.

The following are the steps to capture & decode the voice packets:

- Capturing and Decoding RTP packets. Capture the packets and select **Analyze -> RTP-> Show all streams** options from the wireshark/ethereal interface.
- Analyzing a Session. Select a stream for analyzing & then reassemble.

- Publishing. Open a file and save the audio (.au) stream that contains this captured voice.

This attack looks sometimes difficult because all communication devices restrict broadcast communication. To get success in this attack first we need to use ARP spoofing so that the attacker broadcasts all the spoofed advertisements of the MAC addresses and thus forces the following IP packets to flow through the attacker's host . This will thereby allow the eavesdropping of communications between two legitimate users. The following image is to summarize the ARP spoofing attack.

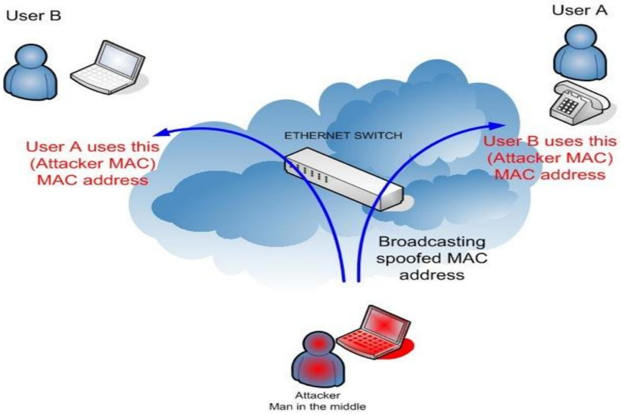
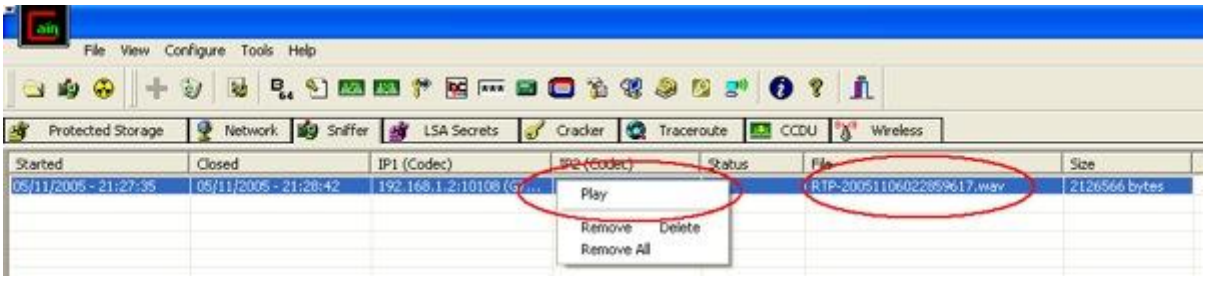

User B
User A
User A uses this (Attacker MAC) MAC address
ETHERNET SWITCH
User B uses this (Attacker MAC) MAC address
Broadcasting spoofed MAC address
Attacker
Man in the middle

Figure 6.7: ARP Spoofing attack

Using ARP spoofing, an attacker is able to capture, analyze and eavesdrop into VoIP communications.

The Figure 6.8 below demonstrates the use of the Cain tool which usually provides the ability to perform the eavesdropping attack and capture VoIP traffic.



Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File	Size
05/11/2005 - 21:27:35	05/11/2005 - 21:28:42	192.168.1.2:10108 (G...			RTP-20051106022859617.wav	2126566 bytes

Figure 6.8: Using Cain to perform a man-in-the-middle attack

Threats

1. It is not limited to VoIP Services.

2. Because VoIP calls are not encrypted, perhaps some encryption option are there such as PKI to using add-ons such a zfone, however there is a layer of incompatibility because there are different platform involved such as desktop, telephones, web and typical phone as well. And in all the systems, there also no easy solution to ensure end to end solution.
3. The encryption is very difficult to implements.
4. Another issue is the number of peers in the conversation such as on mobile, in coffee shop, in restaurant and so on. And the security of also dependent on the security of the coffee shop, their ISP and the other peers in between.

Defense

- Employees must be alert.
- Limited network access must be there to each and every employee inside also and from outside also.
- Continuous supervision or observation should be required to stop this attack.
- It is not limited to VoIP Services.
- Because VoIP calls are not encrypted, perhaps some encryption option are there such as PKI to using add-ons such a zfone, however there is a layer of incompatibility because there are different platform involved such as desktop, telephones, web and typical phone as well. And in all the systems, there also no easy solution to ensure end to end solution.
- The encryption is very difficult to implements.
- Another issue is the number of peers in the conversation such as on mobile, in coffee shop, in restaurant and so on. And the security of also dependent on the security of the coffee shop, their ISP and the other peers in between.

6.2.3 Attack 3: DoS Attack

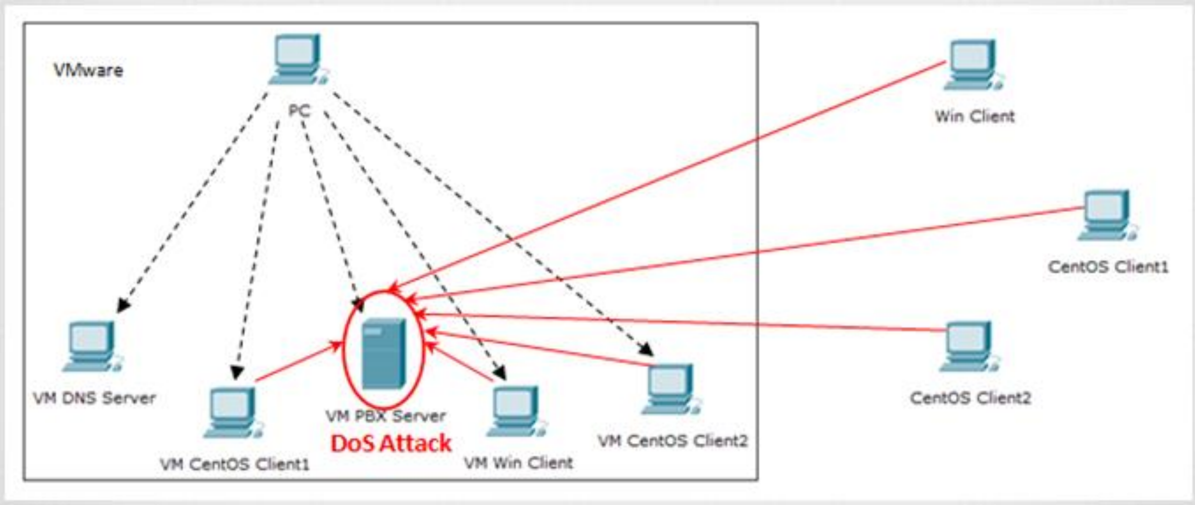


Figure 6.9: Network I used for DoS.

It is almost unwanted flow in a network.

DoS for Exhaustion of Memory

In this case Stateful servers flooded with continues request streams and it will soon run out of memory very easily.

DoS for Exploitation

Brute Force Attack: In this attack, mounting the attack on the memory of the SIP server is to start a large number of SIP sessions with each different session identities.

Broken Sessions

With brute force attack, memory is consumed during time of transaction so to make busy SIP server, just make the illegal request to SIP server and if in case SIP server is not able to resolve the request, the SIP proxy needs to maintain the state for at least 3 minute while it still to re-transmit the message.

Flooding Attacks

It is by a fast stream of INVITE messages with different session identifiers. And it might be from multiple machines.

Malformed Messages

Send continues bulk messages and confuse the SIP servers

Irresolvable DNS attack

In this case, an SIP server facing an irresolvable address in a header field.

DoS Vulnerabilities

- UDP Malformed Packet
- Less User with MD5 Encryption
- Forge INVITE Requests
- Forge SIP Response
- Remote DoS attack to Register Users
- Flooding through Remote DoS

Preventions:

1. **Server Design:** It requires Fast CPUs, large memory module and a very high speed network connection. A server needs fast memory allocation scheme, event handling, and proper parsing mechanism.
2. **Parallel Processing:** To avoid the blocking of incoming messages, if server is busy in processing messages or waiting for the answer of an external server (ex. AAA) a proxy should be implemented using threats or parallel processes where each process or thread is responsible for processing one message at a time.
3. Check if transaction is established or not, if so, absorb.
4. Using the packet's source IP address in order to avoid DNS resolution.
5. If the architecture allows it, authenticate it statelessly in order to avoid the memory exhaustion attack.
6. Check if there is prsence of any viruses.
7. Scan for attack-pattern.
8. Drop all the suspicious packets.
9. Establish the transaction state. This helps you to avoid overburden on server.
10. Use predictive nonce to make sure that REGISTERs are not tampered.
11. Assign quota for each destination address to prevent increase of dividing extension.
12. Deny suspicious contact addresses.

Architecture for Defense:

1. **Entry based host:** This is the point to entry into VoIP Network. At this stage IDS filters clearly malicious messages and update firewall based on operations.
2. **Flooding Defense:** It checks the packet's payloads on servers and also used to resolve message types. And if pre-defined threshold is reached an alert will be generated.
3. **Malicious Message Defense:** It is really very difficult to differentiate between legal and illegal messages. For that message filter might be helpful but not 100% such as Google message filtering BOT

DoS in Detail

1. **Signaling Protocol DoS Attack**
    - In this the message are sent in human readable format means not encrypted.
    - Because of simple form, it would make forwarding faster but not in a safe way.
    - In this case attacker can disrupt the phone call by sending malicious messages to the recipient.
    - Another way to disrupt a phone service is by continually sending it.

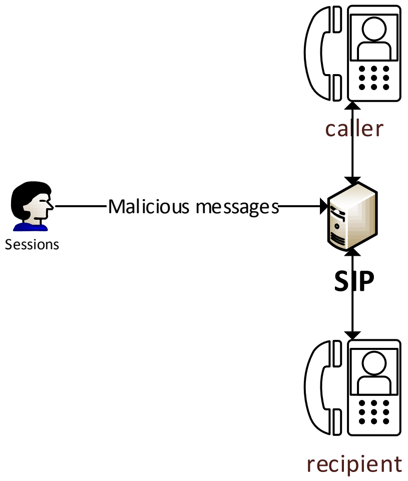


Figure 6.10: SIP Signaling.

Possible attack Solutions

- The network's implementation in a firewall should be between important SIP proxies.
- Packet filter is necessary between SIP servers.
- The whole network framework could be embedded.

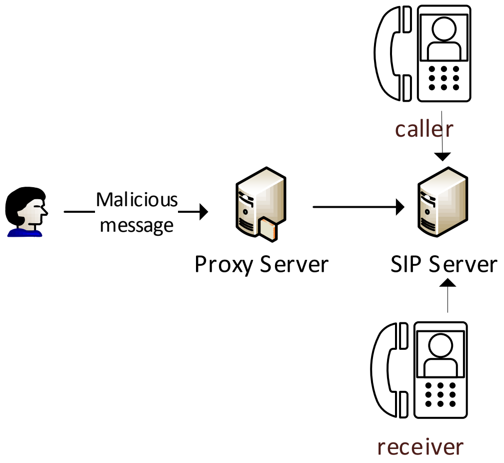


Figure 6.11: Use proxy server to filter malicious messages.

2. **Transport Protocol (RTP) DoS Attack**
   - An outgoing call could be interrupted or disconnected.
   - Or might be it could be with extra noise inserted.
   - It works as a Signaling DoS attack but in this case attackers use noise to disturb network.

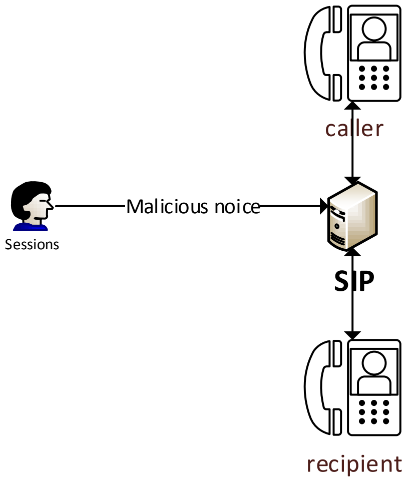


Figure 6.12: Transport Protocol DoS Attack.

Possible attack Solutions

- SRTP might be useful because it is a secure version of RTP protocol but not widely used.
- Proxy server must be used for encryption.

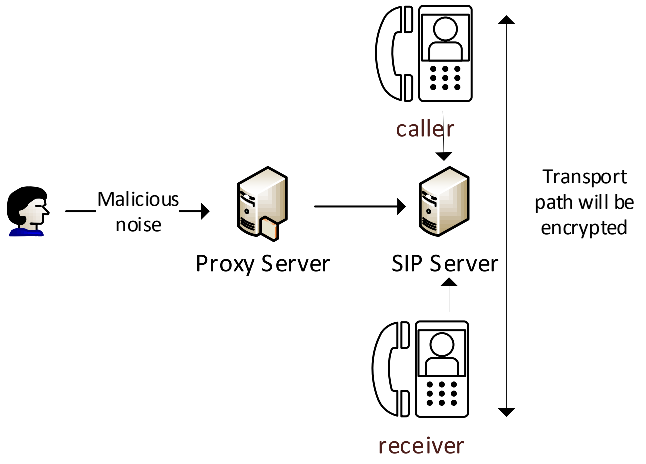


Figure 6.13: Use Proxy to stop extra noise and encrypt existing communication.

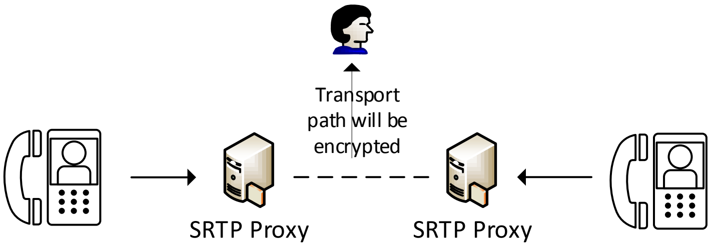


Figure 6.14: Use proxy for encryption between untrusted networks.

3. Flooding DoS Attack

- Means to flood a network with lots of traffic
- So that there is not enough bandwidth for legitimate users.
- And sometime there is not enough resources left for legitimate users.

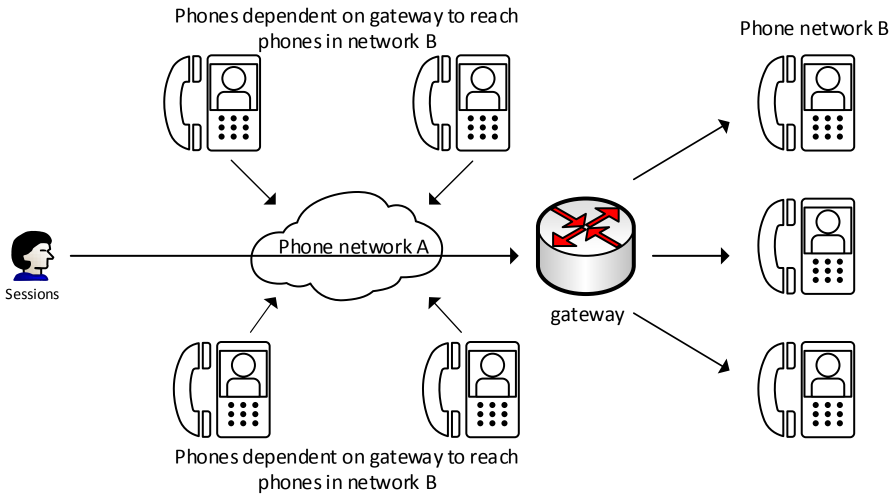

Phones dependent on gateway to reach phones in network B
Phone network B
Phone network A
Sessions
gateway
Phones dependent on gateway to reach phones in network B

Figure 6.15: Network for DoS Flooding.

Possible attack Solutions

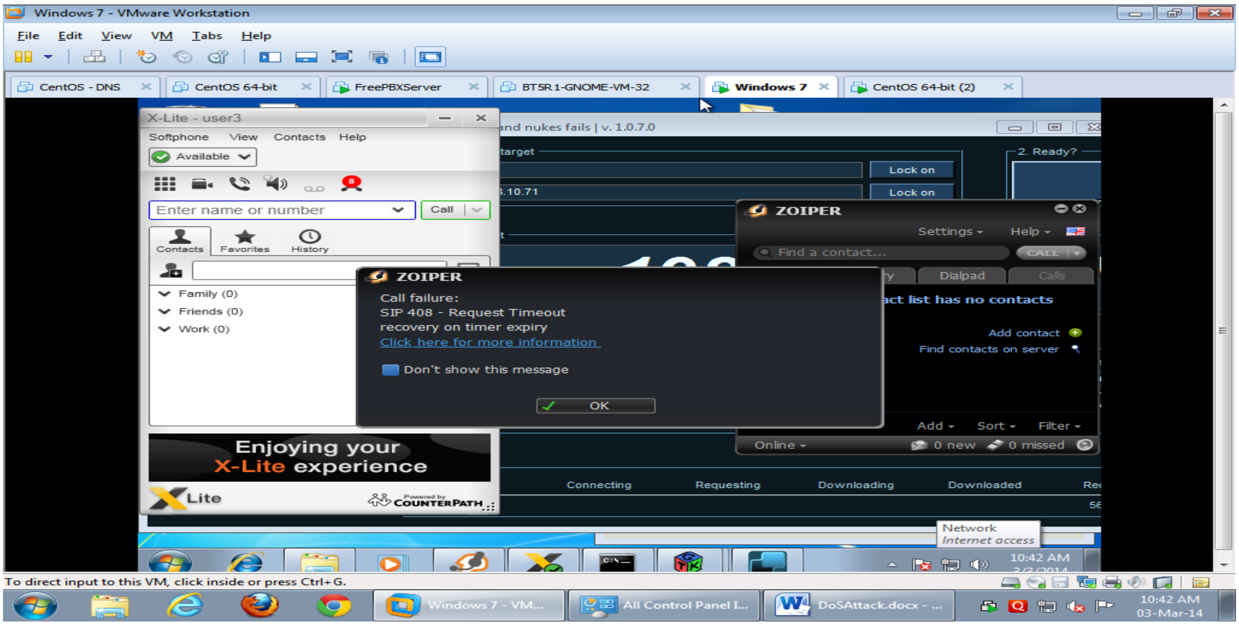
- Not 100% possible to solve but Implement QoS based filtering by routers. In this way, VoIP can be given more priority or bandwidth.

4. **Gateway DoS Attack**

- In this kind of network, to allow phone calls between two different networks and for that special gateways have been set up that are able to process VoIP calls.
- These gateways have limited resources because they are connected two both VoIP and traditional phone networks which can cause gateways to easily run out of the resources.
- Means all calls would pass through gateway so the only the number of concurrent calls are possible and at one point, the gateway will stop accepting calls.
- This is the way, a gateway can very easily be loaded causing DoS for legitimate users.

Possible attack Solutions

- Not possible till we have traditional phone networks in a working condition.



ZOIPER

Call failure:
SIP 408 - Request Timeout
recovery on timer expiry
Click here for more information

□ Don't show this message

OK

Figure 6.16: Screenshot DoS Flooding.

6.2.4 Attack 4: VoIP SPIT (Spam over Internet) Attack

1. Spam in the most unwanted traffic in the internet.
2. SPIT is just like a spam.
3. It uses voice messages instead of text messages.

4. It is a major threat in IP telephony.
5. Sometime it is greater than a normal SPAM attack.
6. In case of attack, pre-recorded message is played after the call is answered.

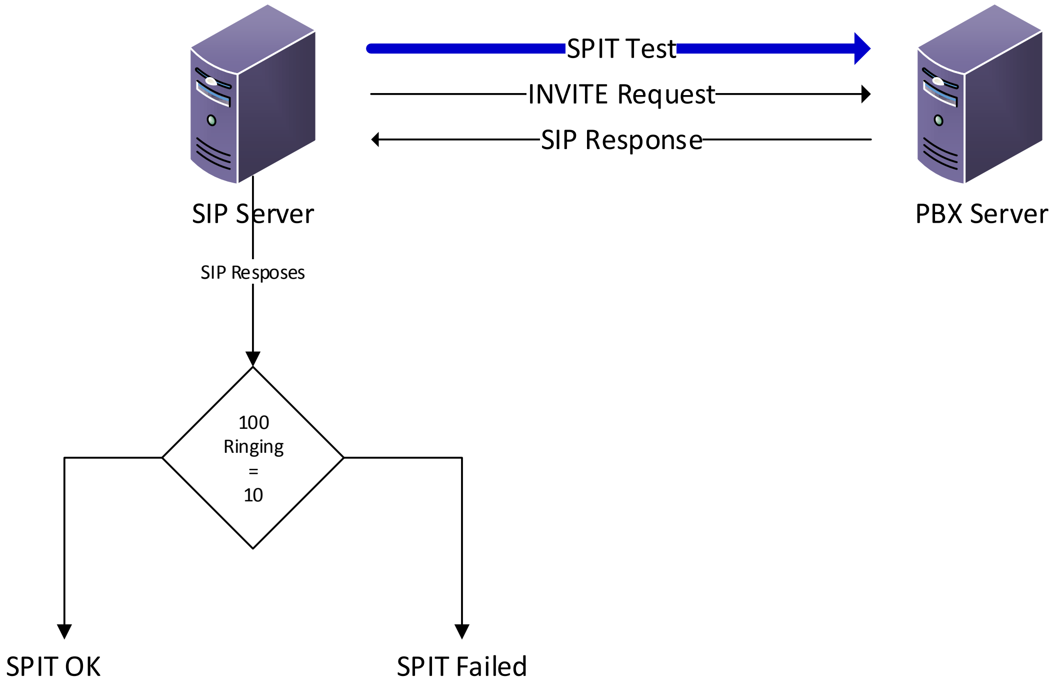


Figure 6.17: Working of SPIT Attack.

How this attack is done:

1. An attacker enters value of valid accounts of 101 (victim) and 102 (originator) with its password.
2. Then SPITFILES ties to register them into SIP server as account 102 and initiate a call to 101.
3. And the system detects successfully connection between both and getting response from SIP server.
4. Now SIP server performs 10 continues call.
5. And all responses from SIP server must be 100 ringing.

Prevention

1. Caller identity must be compared with stored identities called blacklist filtering.
2. In case of first time call, a system asks to call again if a caller calls again, a system puts it into whitelist.

3. Meet the requirement of proper firewall setting.
4. When caller calls, a sender domain must be identified but this system does not exist yet.
5. Speech recognition techniques must be implemented to identify original caller.
6. VSP (VoIP Service Provider) must have call records details to classify the spam calls.
7. IP address of a call must be identified.
8. Probability of arriving of all must be filtered and watched.
9. Inter-domain trust must be defined so other domain can’t interfere into it.
10. Check if caller often change its SIP identification.
11. In most cases spam caller is automated system so quest must be asked to a caller to identify whether it is human being or not.
12. Call repetitive rate must be controlled such as if a caller calls someone up to two minutes continuously, in this case a caller must be blocked temporarily.

6.2.5 Attack 5: VoIP Spoofing

1. It is basically used for fake calls for any reason.
2. Display victim caller id on recipient's machine or phone.
3. Victim is not able to know that which one is using its caller id and where?
4. Even some time, some vendors provide this service.

Symptoms of attack

1. Caller name is blindly passed to the called party.
2. Name is generated by the telephone company.

Only geographic location is displayed on a device.

Prevention

1. Websites must be blocked which provides caller-id spoofing services.
2. Access service provides must be alert.
3. If call spoofing is required then third party permission must be required.

Legal use of call spoofing

1. In large enterprise, if it has 5000 employees and one special no such as 510-11111 so instead of giving different extension to all branches, there will be a single extension so any one can identify that the call is from this enterprise.
2. In case of Toll-Free telephone no.
3. In case of when call center calls to its clients.
4. Automatic answering service for marketing or provide information or for alerting.
5. Google Voice is the best example because it display same no on a machine or phone.
6. Emergency no such as 100 for police, 101 for fire brigade, 108 for ambulance in Gujarat (India).

6.2.6 Attack 6: VoIP Call Flooding

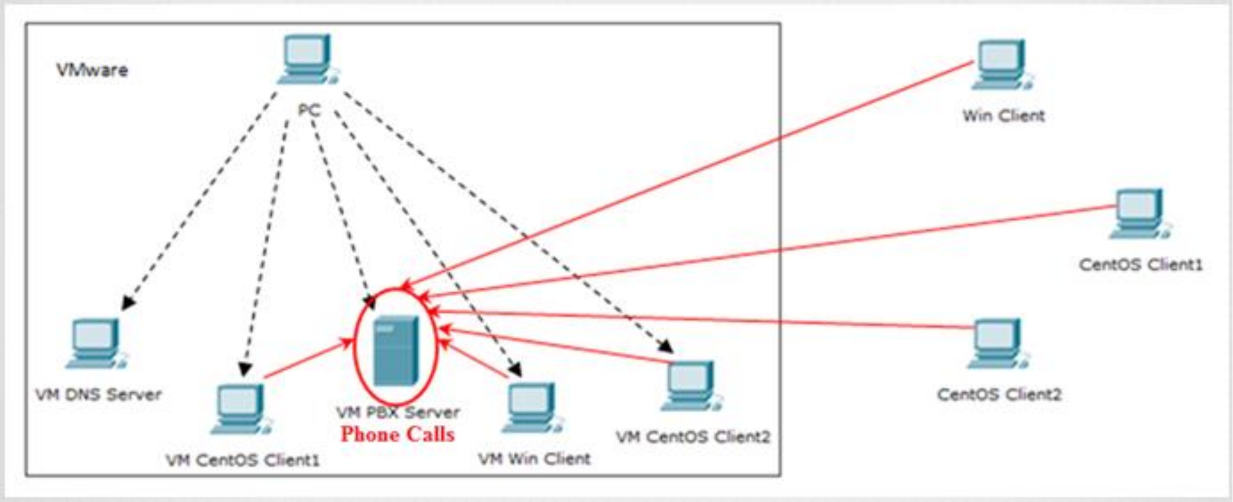


Figure 6.18: Network I used for Call Flooding.

1. It is a part of DoS Attack
2. In this case, the attacker floods valid or invalid heavy signals or data to a target system.
3. So it reduces performance of a targeted system.
4. Valid or invalid call request in bulk.
5. Ping flooding

Types of VoIP Flooding

1. Flooding with Registrar: In this attack, an attacker sends bulk request to register it into SIP server so other genuine user cannot be able to register because system will be responded.
2. Flooding with Proxy Server: In this attack, an attacker develops distributed INVITE flood and then attack.

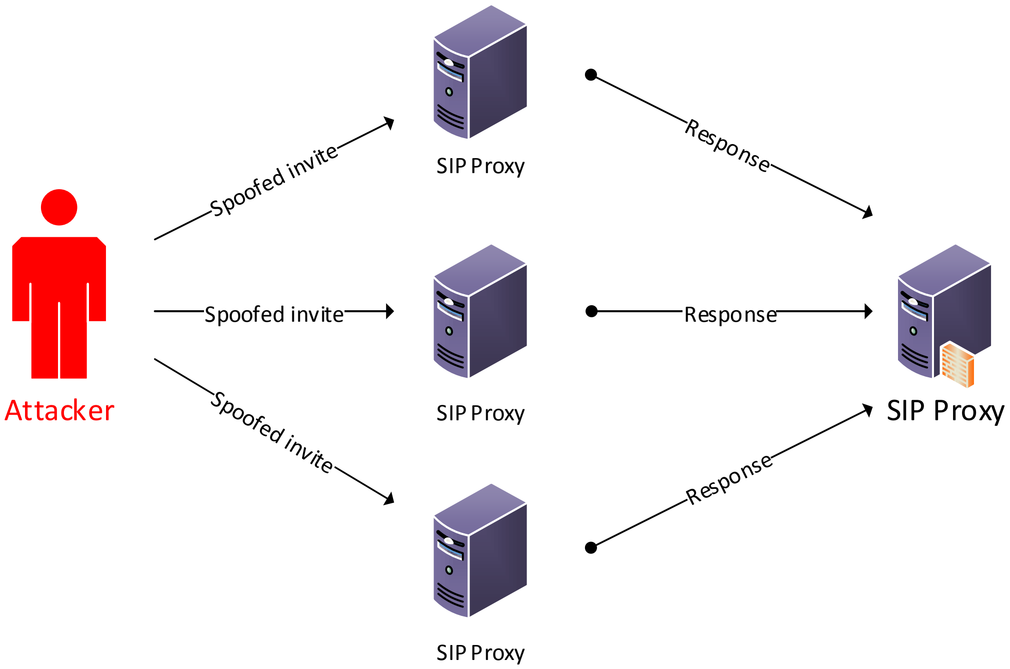


Figure 6.19: Flooding with Proxy Server.

3. Flooding with End User: It is very easy attack to perform because when an attacker makes only 10 to 15 calls to a victim, a victim's system will not be able to respond.

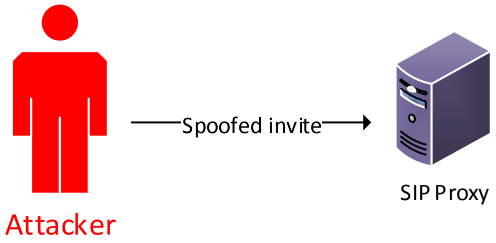


Figure 6.20: Flooding with End User.

Prevention

1. A traffic monitoring system must be implemented.
2. Session filtering must be implemented to watch which sessions were not uncompleted.
3. Flooding detection module must be implemented.

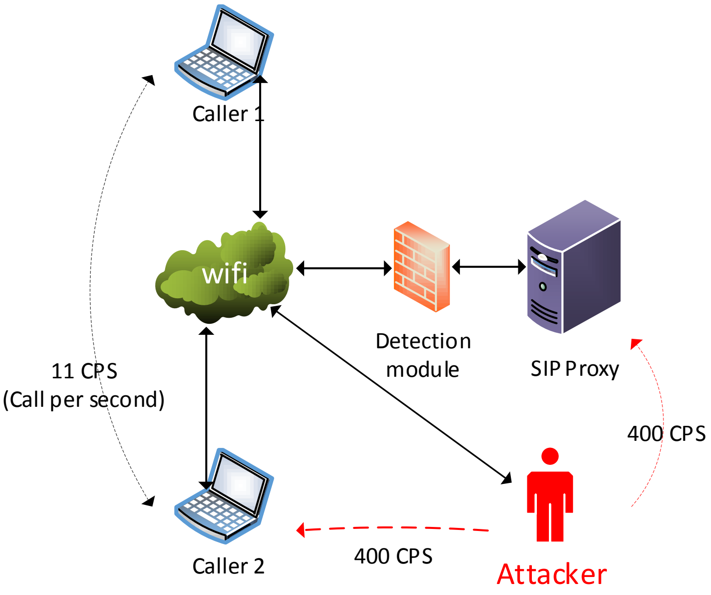
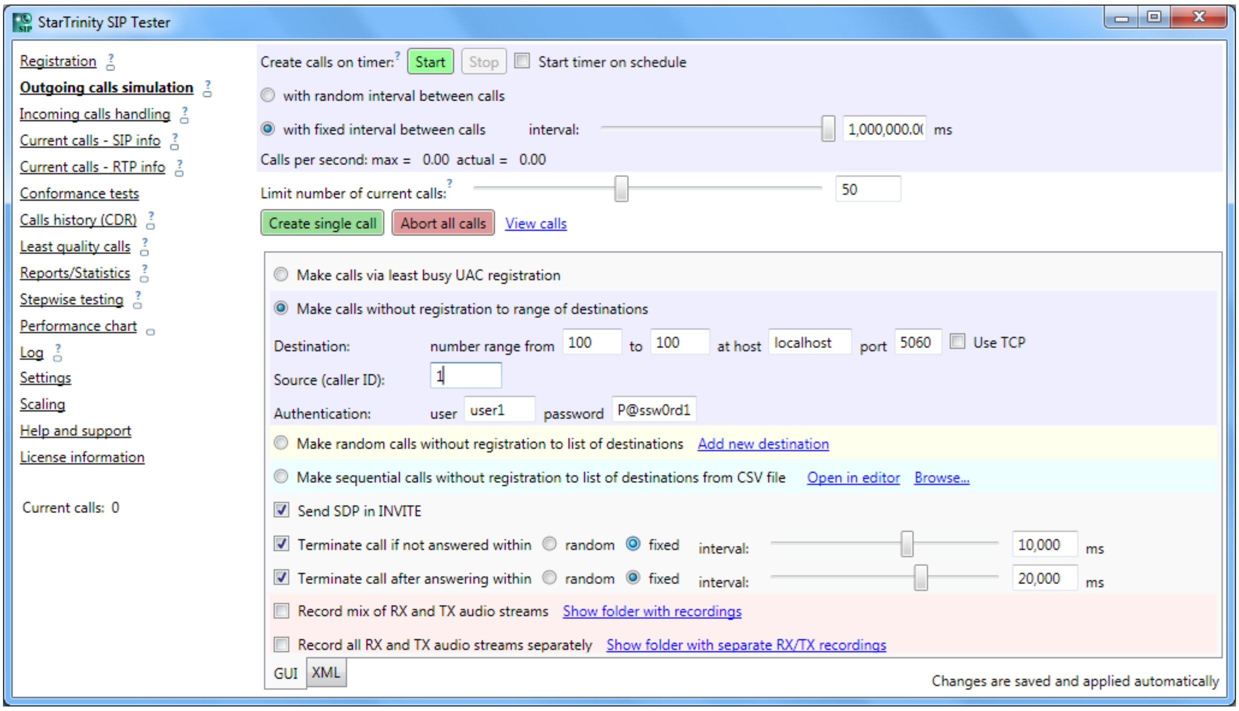


Figure 6.21: Prevention for Call Flooding.



Current calls: 0

Create calls on timer: □ Start timer on schedule

○ with random interval between calls

● with fixed interval between calls interval: 1,000,000.0(ms

Calls per second: max = 0.00 actual = 0.00

Limit number of current calls: 50

○ Make calls via least busy UAC registration

● Make calls without registration to range of destinations

Destination: number range from 100 to 100 at host localhost port 5060 □ Use TCP

Source (caller ID): 1

Authentication: user user1 password P@ssw0rd1

○ Make random calls without registration to list of destinations

○ Make sequential calls without registration to list of destinations from CSV file

☑ Send SDP in INVITE

☑ Terminate call if not answered within ○ random ● fixed interval: 10,000 ms

☑ Terminate call after answering within ○ random ● fixed interval: 20,000 ms

□ Record mix of RX and TX audio streams

□ Record all RX and TX audio streams separately

Changes are saved and applied automatically

Figure 6.22: Screenshot for Call Flooding Software.

6.2.7 Attack 7: VoIP Fuzzing

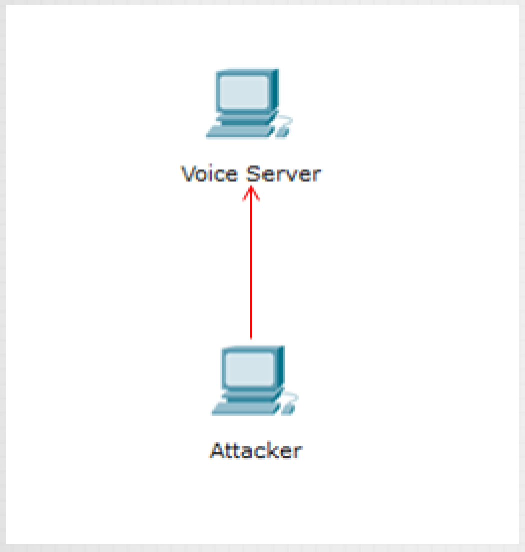


Figure 6.23: Network I used for VoIP Fuzzing.

Basically Fuzzing tools were not created for hacking but they were created for testing VoIP networks from dummy packets. But an attackers use this tools for attacks. It is a one kind of DoS attack.

1. Through this tool you can generate dummy request.
2. You can generate request using loop also.
3. You can generate and send large dummy packets to busy communication traffic.
4. At different level, you can do this attack as follow…
    a. SIP INVITE
    b. SIP ACK
    c. SIP CANCEL
    d. SIP Request Framework

This is the most dangerous attack in the world of VoIP. The impacts of this attack are as follows…

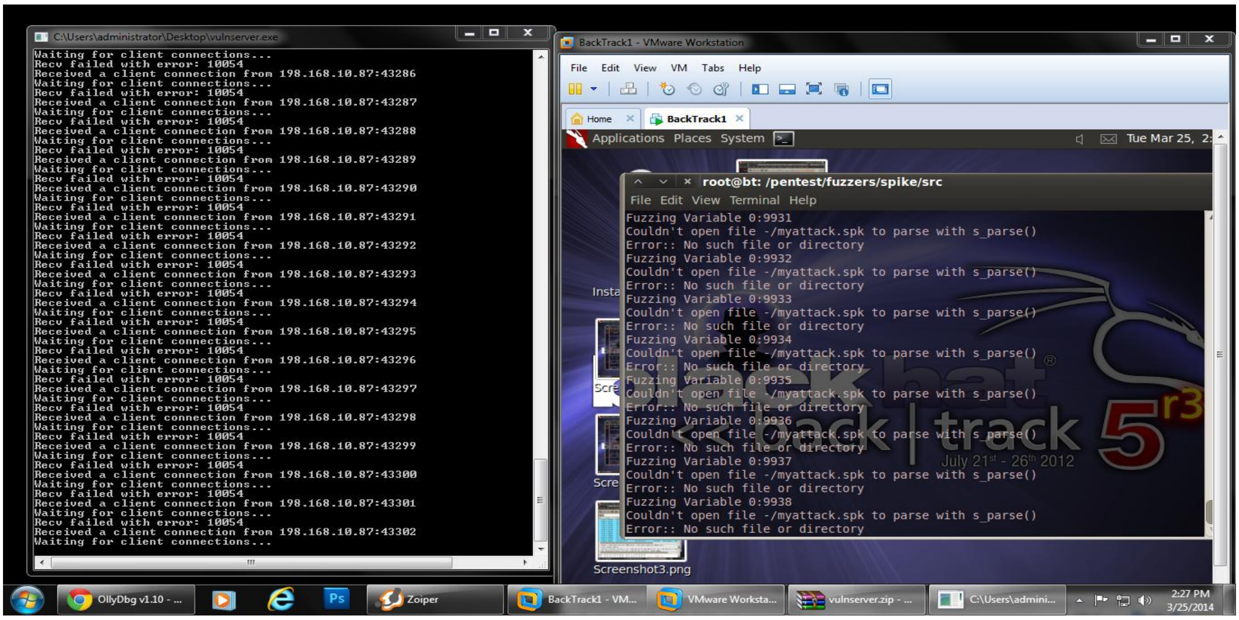
1. Loop attack
2. Memory Overflow
3. State Killing
4. Traffic Jam
5. System Crash or Software Crash

Vulnerabilities for this attack:

1. Because the most VoIP protocols are public and less secure.
2. Fuzzing tool are too easy to use even for non-programmer also.
3. Difficult to test all dummy packets.

Prevention

As par DoS prevention, because there is no any perfect prevention method for this attack.



```
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43286
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43287
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43288
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43289
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43290
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43291
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43292
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43293
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43294
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43295
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43296
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43297
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43298
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43299
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43300
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43301
Waiting for client connections...
Recv failed with error: 10054
Received a client connection from 198.168.10.87:43302
Waiting for client connections...
```

BackTrack1 - VMware Workstation
File Edit View VM Tabs Help
Home
BackTrack1
Applications Places System
Tue Mar 25, 2:
root@bt: /pentest/fuzzers/spike/src
File Edit View Terminal Help

```
Fuzzing Variable 0:9931
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9932
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9933
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9934
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9935
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9936
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9937
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
Fuzzing Variable 0:9938
Couldn't open file -/myattack.spk to parse with s_parse()
Error:: No such file or directory
```

Figure 6.24: Screenshot for Fuzzing.

6.2.8 Attack 8: VoIP Phishing

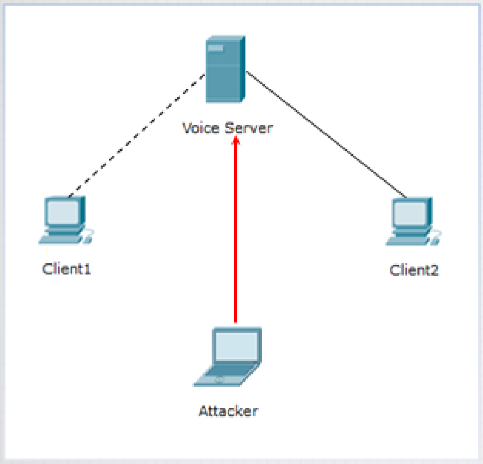


Figure 6.25: Network I used for VoIP Phishing.

Phishing is just to get someone’s confidential data and use it illegally and it is VoIP phishing so called: Vhishing.

Working of Vhishing

1. Very popular attack.
2. There is no any technical knowledge required to perform this attack. Only better communication skill is required to attract victims’ attention.
3. In this attack, an attacker sends a forge mail or fake call and it seems an official message from a company. And an attackers demands victims’ confidential data.
4. And some victims’ easily give it to an attacker. Then an attacker uses for an illegal transactions.
5. Most of the attackers use VoIP but not PSTN to do VoIP attack because PSTN is more secure and easily traceable.

Phishing Attacks’ Examples

Here are examples of ways in which you can be attacked if you are a phishing target:

1. Get an email from Banks, financial institutions and PayPal to inform some irregularity on your account and you are told to activate that account after giving some personal details.

2. Get a fake voice call from Internet and say that someone is trying to change your password so please give us your information to secure your account.

3. Get a call from your bank and say that suspicious activities on bank account, and tell you to give banking details to secure your bank account.

How VoIP Makes Phishing Easier

- It is cheaper than PSTN and widely used.
- Caller ID has been easily tempered.
- Asterisk is popular open source VoIP software and it gives so much flexibility to the programmer, persons with low skills can achieve illegal tasks. Anyone with basic knowledge of VoIP can change its deployment and make a group of dummy numbers that they can use victims’ account without changing their own identities.
- VoIP devices and softphones are very portable and could be taken anywhere.

- Easy to integrate VoIP hardware with PCs and it makes easy for attackers to hack phone calls.
- VoIP phone no can be easily set up and destroyed
- Attackers can send thousand message or call at one time
- In VoIP, Virtual Number can be created very easily by an attacker.

Prevention From Vhishing Attacks

- Follow your bank's or company's policy on sending messages or calls
- Avoid calls or messages starts from "5000".
- Never reply to a doubtful text messages or calls without verifying.
- Block texts from the internet, features are provided by providers.
- Never give sensitive information to automated call system.
- Use anti-phishing system with PBX server to filter doubtful calls.
- If you have been hacked then report it to reportphishing@antiphishing.org.
- Make aware your friends.

6.2.9 Toll Fraud

1. It is the most likely to make the news.
2. A very high dollar value can be placed on toll fraud.
3. It is often the most important in the eyes of a large organizations.
4. A successful theft of service from a large organization can go unnoticed for quite some time, allow the attacker to rack up a large bill at the organizations expense.
5. Quite easy to accomplish because of simple configuration problems in a dial plan.
6. These issues are often difficult to identify.
7. Very profitable from the point of view of the attacker to commit toll fraud as once the attack is complete there are no real costs involved and the attacker can abuse the services quite rapidly.

6.2.10 Password Attack

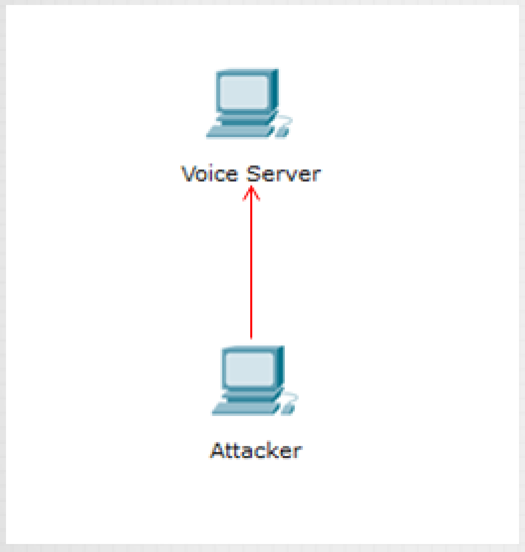
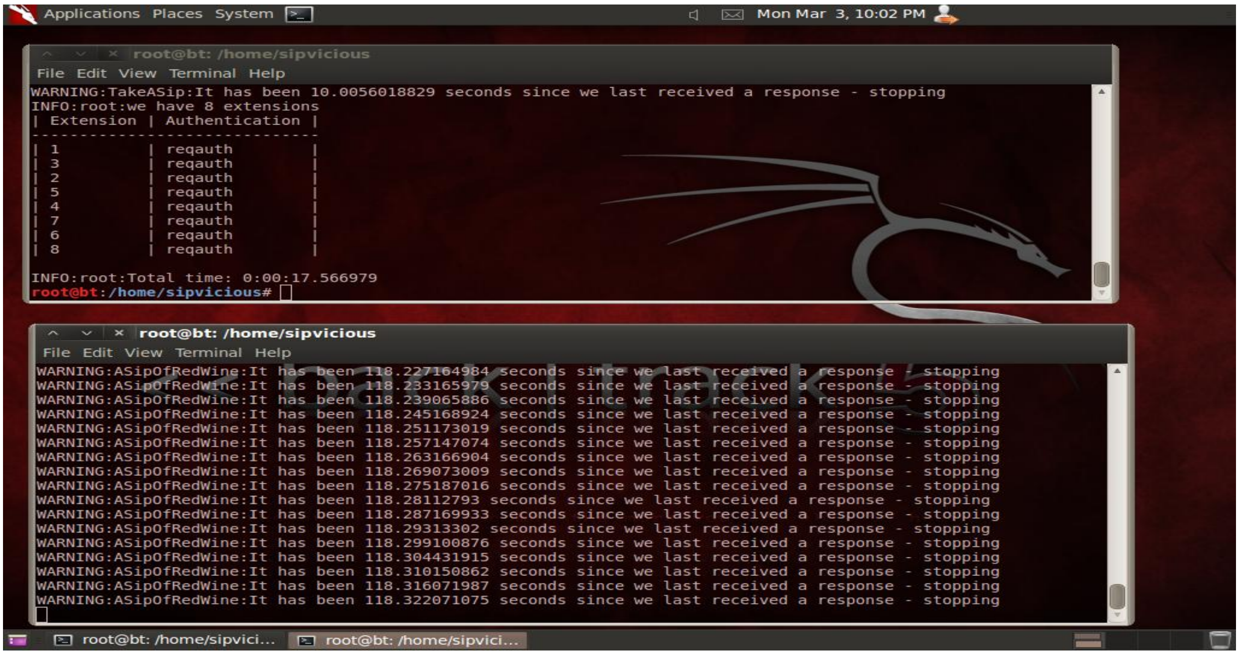


Figure 6.26: Network I used for Password Attack.

In this attack the attacker changes the password of legitimate user and gains access to his/her account. The password is set same as the user Id in this attack.

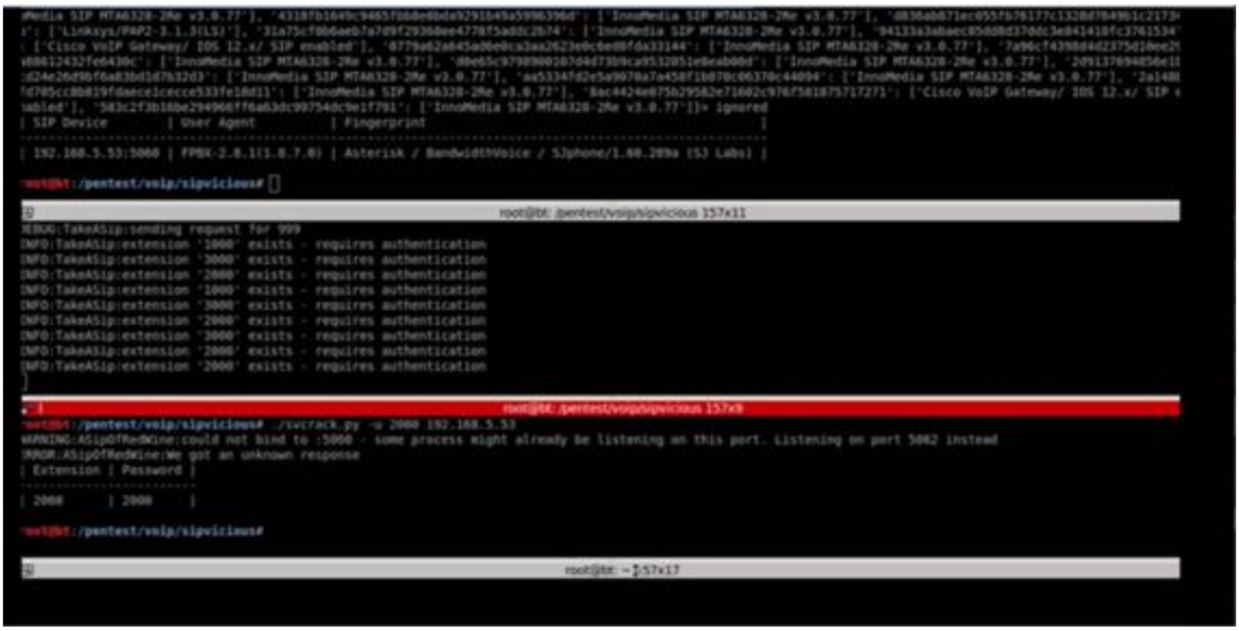
Same Network but Trixbox & BackTrack used.


Applications Places System
Mon Mar 3, 10:02 PM
root@bt: /home/sipvicious
File Edit View Terminal Help
root@bt: /home/sipvicious
File Edit View Terminal Help
root@bt: /home/sipvici...
root@bt: /home/sipvici...

```
WARNING:TakeASip:It has been 10.0056018829 seconds since we last received a response - stopping
INFO:root:we have 8 extensions
| Extension | Authentication |
------------------------------
| 1         | reqauth        |
| 3         | reqauth        |
| 2         | reqauth        |
| 5         | reqauth        |
| 4         | reqauth        |
| 7         | reqauth        |
| 6         | reqauth        |
| 8         | reqauth        |

INFO:root:Total time: 0:00:17.566979
root@bt:/home/sipvicious#
```

```
WARNING:ASipOfRedWine:It has been 118.227164984 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.233165979 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.239065886 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.245168924 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.251173019 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.257147074 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.263166904 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.269073009 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.275187016 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.28112793 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.287169933 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.29313302 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.299100876 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.304431915 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.310150862 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.316071987 seconds since we last received a response - stopping
WARNING:ASipOfRedWine:It has been 118.322071075 seconds since we last received a response - stopping
```

Figure 6.27: Screenshot of failed Password Attack.



```
#Media SIP MTA6328-2Re v3.0.77'], '4318fb1649c9465fb6de6bda9291b49a5996396d': ['InnoMedia SIP MTA6328-2Re v3.0.77'], 'd836ab871ec055fb76177c1328d7849b1c2173
r': ['Linksys/PAP2-3.1.3(LS)'], '31a75cf006aeb7a7d9f29368ee4778f5addc2b74': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '94133a3abaec05dd0d37ddc3e841410fc3761534'
: ['Cisco VoIP Gateway/ IOS 12.x/ SIP enabled'], '0779a62a845ad6e0ca3aa2623e0c6ed8fda33144': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '7a96cf4398d4d2375d10ee2
a88612432fe6430c': ['InnoMedia SIP MTA6328-2Re v3.0.77'], 'd0e65c9798980207d4d73b9ca9532851e0eab00d': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '2d91376948856e1
:d24e26d9bf6a83bd1d7b32d3': ['InnoMedia SIP MTA6328-2Re v3.0.77'], 'aa5334fd2e5a9070a7a458f1b070c06370c44094': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '2a148
fd705cc8b819fdaece1cecce533fe10d11': ['InnoMedia SIP MTA6328-2Re v3.0.77'], '8ac4424e075b29582e71602c976f5818757717271': ['Cisco VoIP Gateway/ IOS 12.x/ SIP e
abled'], '583c2f3b16be294966ff6a63dc99754dc9e1f791': ['InnoMedia SIP MTA6328-2Re v3.0.77']}> ignored
| SIP Device        | User Agent          | Fingerprint                                      |
------------------------------------------------------------------------------------------------
| 192.168.5.53:5060 | FPBX-2.8.1(1.8.7.0) | Asterisk / BandwidthVoice / SJphone/1.60.289a (SJ Labs) |

root@bt:/pentest/voip/sipvicious# 
```

root@bt: /pentest/voip/sipvicious 157x11

```
DEBUG:TakeASip:sending request for 999
INFO:TakeASip:extension '1000' exists - requires authentication
INFO:TakeASip:extension '3000' exists - requires authentication
INFO:TakeASip:extension '2000' exists - requires authentication
INFO:TakeASip:extension '1000' exists - requires authentication
INFO:TakeASip:extension '3000' exists - requires authentication
INFO:TakeASip:extension '2000' exists - requires authentication
INFO:TakeASip:extension '3000' exists - requires authentication
INFO:TakeASip:extension '2000' exists - requires authentication
INFO:TakeASip:extension '2000' exists - requires authentication
```

root@bt: /pentest/voip/sipvicious 157x9

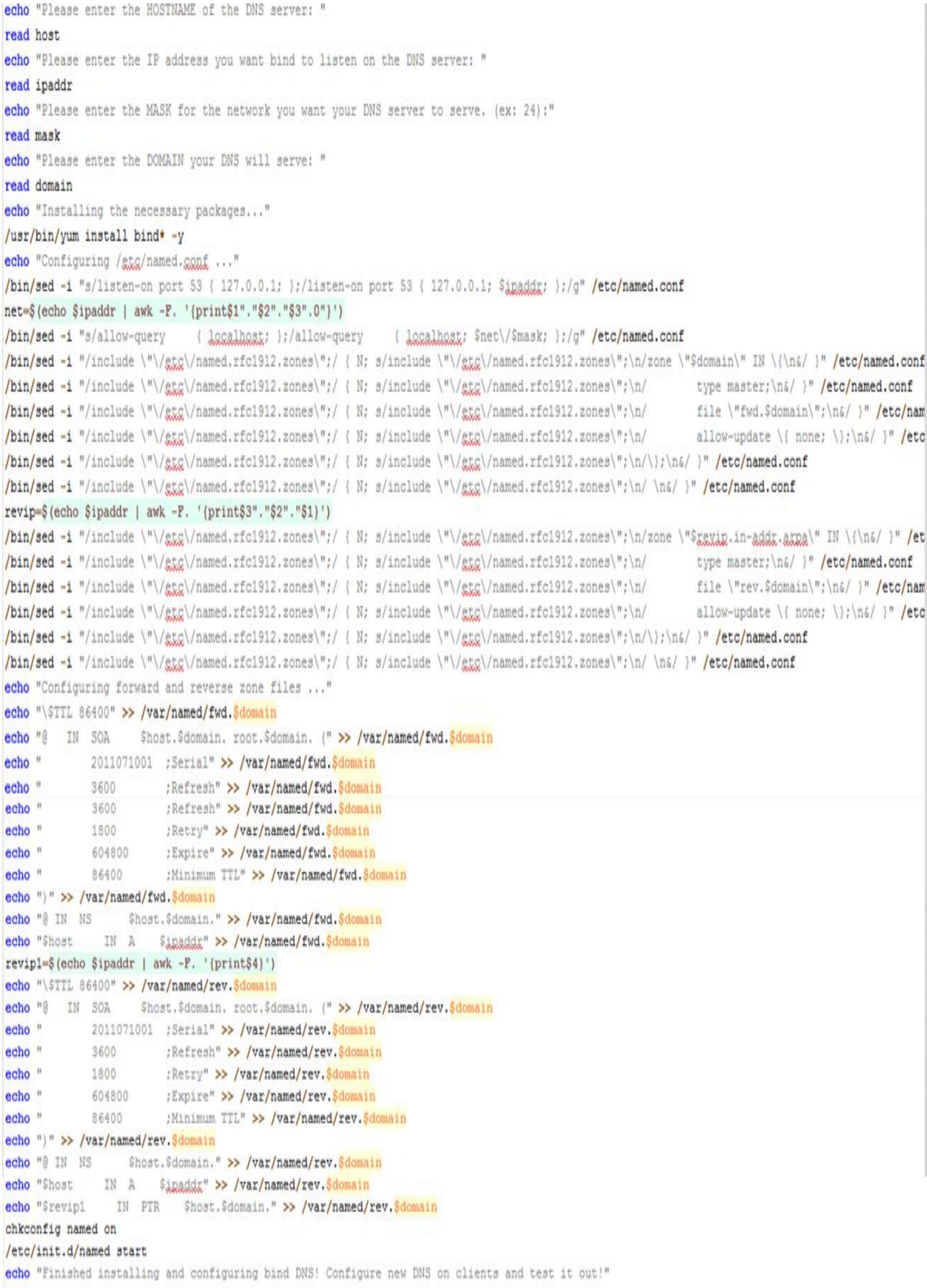
```
root@bt:/pentest/voip/sipvicious# ./svcrack.py -u 2000 192.168.5.53
WARNING:ASipOfRedWine:could not bind to :5060 - some process might already be listening on this port. Listening on port 5062 instead
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| 2000      | 2000     |

root@bt:/pentest/voip/sipvicious#
```

root@bt: ~ 157x17

Figure 6.28: Screenshot of successfull Password Attack.

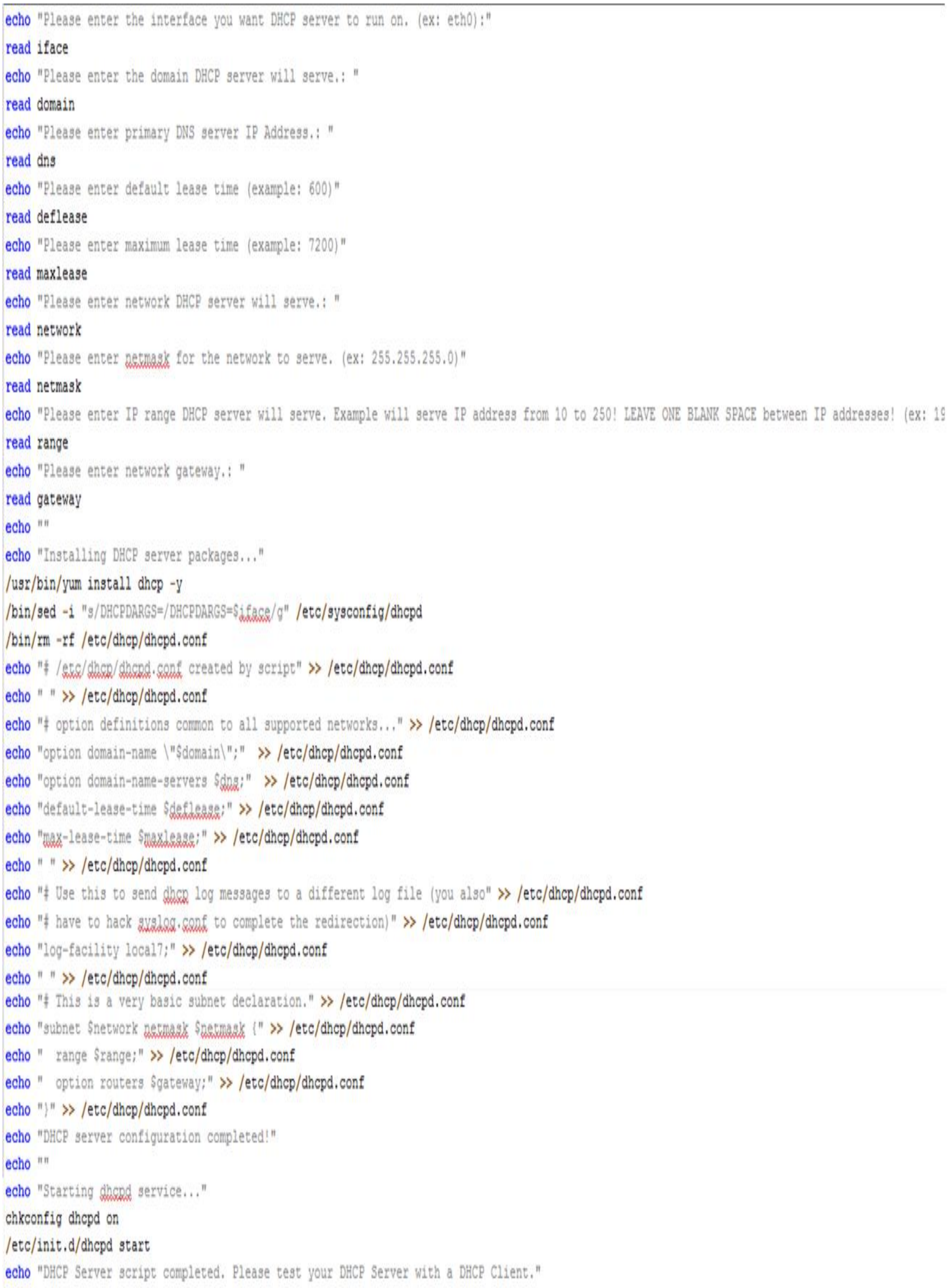
6.3 Network Setup

6.3.1 DNS Script



```
echo "Please enter the HOSTNAME of the DNS server: "
read host
echo "Please enter the IP address you want bind to listen on the DNS server: "
read ipaddr
echo "Please enter the MASK for the network you want your DNS server to serve. (ex: 24):"
read mask
echo "Please enter the DOMAIN your DNS will serve: "
read domain
echo "Installing the necessary packages..."
/usr/bin/yum install bind* -y
echo "Configuring /etc/named.conf ..."
/bin/sed -i "s/listen-on port 53 { 127.0.0.1; };/listen-on port 53 { 127.0.0.1; $ipaddr; };/g" /etc/named.conf
net=$(echo $ipaddr | awk -F. '{print$1"."$2"."$3".0"}')
/bin/sed -i "s/allow-query     { localhost; };/allow-query     { localhost; $net\/$mask; };/g" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/zone \"$domain\" IN \{\n&/ }" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        type master;\n&/ }" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        file \"fwd.$domain\";\n&/ }" /etc/nam
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        allow-update \{ none; \};\n&/ }" /etc
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/\};\n&/ }" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/ \n&/ }" /etc/named.conf
revip=$(echo $ipaddr | awk -F. '{print$3"."$2"."$1}')
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/zone \"$revip.in-addr.arpa\" IN \{\n&/ }" /et
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        type master;\n&/ }" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        file \"rev.$domain\";\n&/ }" /etc/nam
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/        allow-update \{ none; \};\n&/ }" /etc
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/\};\n&/ }" /etc/named.conf
/bin/sed -i "/include \"\/etc\/named.rfc1912.zones\";/ { N; s/include \"\/etc\/named.rfc1912.zones\";\n/ \n&/ }" /etc/named.conf
echo "Configuring forward and reverse zone files ..."
echo "\$TTL 86400" >> /var/named/fwd.$domain
echo "@   IN  SOA     $host.$domain. root.$domain. (" >> /var/named/fwd.$domain
echo "        2011071001  ;Serial" >> /var/named/fwd.$domain
echo "        3600        ;Refresh" >> /var/named/fwd.$domain
echo "        3600        ;Refresh" >> /var/named/fwd.$domain
echo "        1800        ;Retry" >> /var/named/fwd.$domain
echo "        604800      ;Expire" >> /var/named/fwd.$domain
echo "        86400       ;Minimum TTL" >> /var/named/fwd.$domain
echo ")" >> /var/named/fwd.$domain
echo "@ IN  NS      $host.$domain." >> /var/named/fwd.$domain
echo "$host     IN  A     $ipaddr" >> /var/named/fwd.$domain
revip1=$(echo $ipaddr | awk -F. '{print$4}')
echo "\$TTL 86400" >> /var/named/rev.$domain
echo "@   IN  SOA     $host.$domain. root.$domain. (" >> /var/named/rev.$domain
echo "        2011071001  ;Serial" >> /var/named/rev.$domain
echo "        3600        ;Refresh" >> /var/named/rev.$domain
echo "        1800        ;Retry" >> /var/named/rev.$domain
echo "        604800      ;Expire" >> /var/named/rev.$domain
echo "        86400       ;Minimum TTL" >> /var/named/rev.$domain
echo ")" >> /var/named/rev.$domain
echo "@ IN  NS      $host.$domain." >> /var/named/rev.$domain
echo "$host     IN  A     $ipaddr" >> /var/named/rev.$domain
echo "$revip1     IN  PTR     $host.$domain." >> /var/named/rev.$domain
chkconfig named on
/etc/init.d/named start
echo "Finished installing and configuring bind DNS! Configure new DNS on clients and test it out!"
```

6.3.2 DHCP Script



```
echo "Please enter the interface you want DHCP server to run on. (ex: eth0):"
read iface
echo "Please enter the domain DHCP server will serve.: "
read domain
echo "Please enter primary DNS server IP Address.: "
read dns
echo "Please enter default lease time (example: 600)"
read deflease
echo "Please enter maximum lease time (example: 7200)"
read maxlease
echo "Please enter network DHCP server will serve.: "
read network
echo "Please enter netmask for the network to serve. (ex: 255.255.255.0)"
read netmask
echo "Please enter IP range DHCP server will serve. Example will serve IP address from 10 to 250! LEAVE ONE BLANK SPACE between IP addresses! (ex: 19
read range
echo "Please enter network gateway.: "
read gateway
echo ""
echo "Installing DHCP server packages..."
/usr/bin/yum install dhcp -y
/bin/sed -i "s/DHCPDARGS=/DHCPDARGS=$iface/g" /etc/sysconfig/dhcpd
/bin/rm -rf /etc/dhcp/dhcpd.conf
echo "# /etc/dhcp/dhcpd.conf created by script" >> /etc/dhcp/dhcpd.conf
echo " " >> /etc/dhcp/dhcpd.conf
echo "# option definitions common to all supported networks..." >> /etc/dhcp/dhcpd.conf
echo "option domain-name \"$domain\";"  >> /etc/dhcp/dhcpd.conf
echo "option domain-name-servers $dns;"  >> /etc/dhcp/dhcpd.conf
echo "default-lease-time $deflease;" >> /etc/dhcp/dhcpd.conf
echo "max-lease-time $maxlease;" >> /etc/dhcp/dhcpd.conf
echo " " >> /etc/dhcp/dhcpd.conf
echo "# Use this to send dhcp log messages to a different log file (you also" >> /etc/dhcp/dhcpd.conf
echo "# have to hack syslog.conf to complete the redirection)" >> /etc/dhcp/dhcpd.conf
echo "log-facility local7;" >> /etc/dhcp/dhcpd.conf
echo " " >> /etc/dhcp/dhcpd.conf
echo "# This is a very basic subnet declaration." >> /etc/dhcp/dhcpd.conf
echo "subnet $network netmask $netmask {" >> /etc/dhcp/dhcpd.conf
echo "  range $range;" >> /etc/dhcp/dhcpd.conf
echo "  option routers $gateway;" >> /etc/dhcp/dhcpd.conf
echo "}" >> /etc/dhcp/dhcpd.conf
echo "DHCP server configuration completed!"
echo ""
echo "Starting dhcpd service..."
chkconfig dhcpd on
/etc/init.d/dhcpd start
echo "DHCP Server script completed. Please test your DHCP Server with a DHCP Client."
```

Chapter 7

Secured VoIP Network Design

7.1 Network Design & Secure Protocol

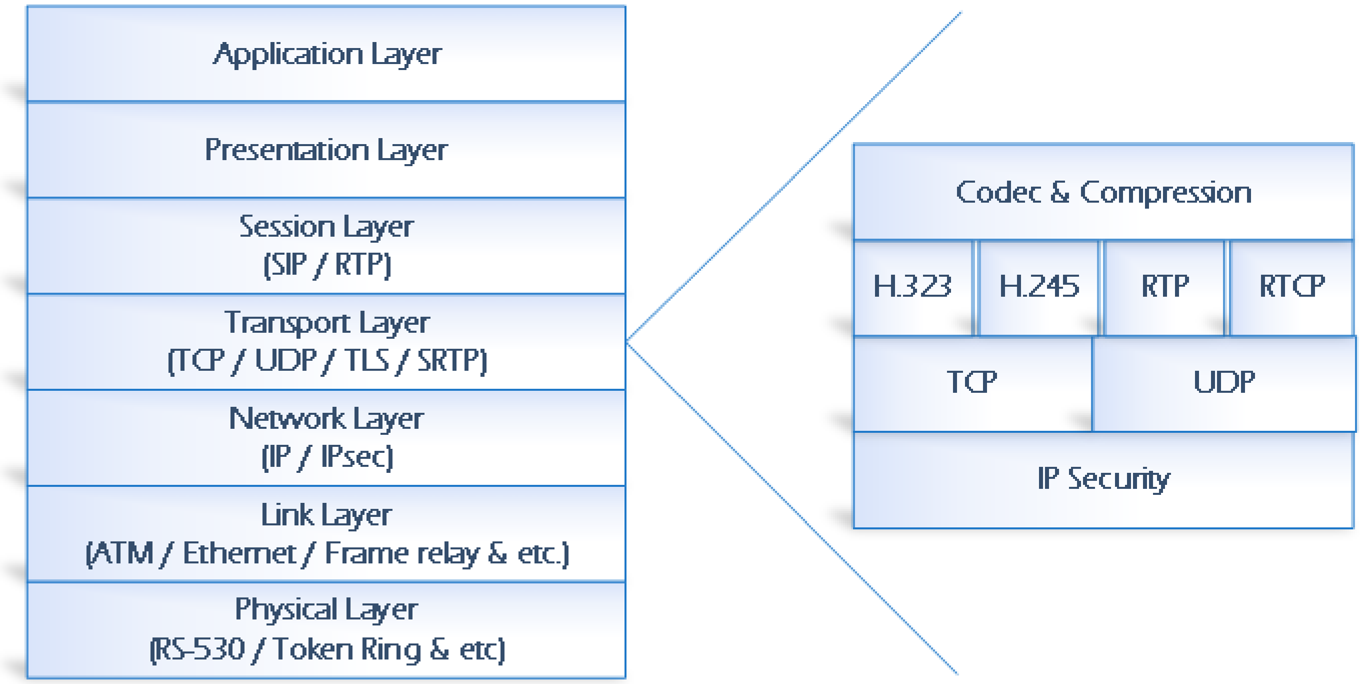


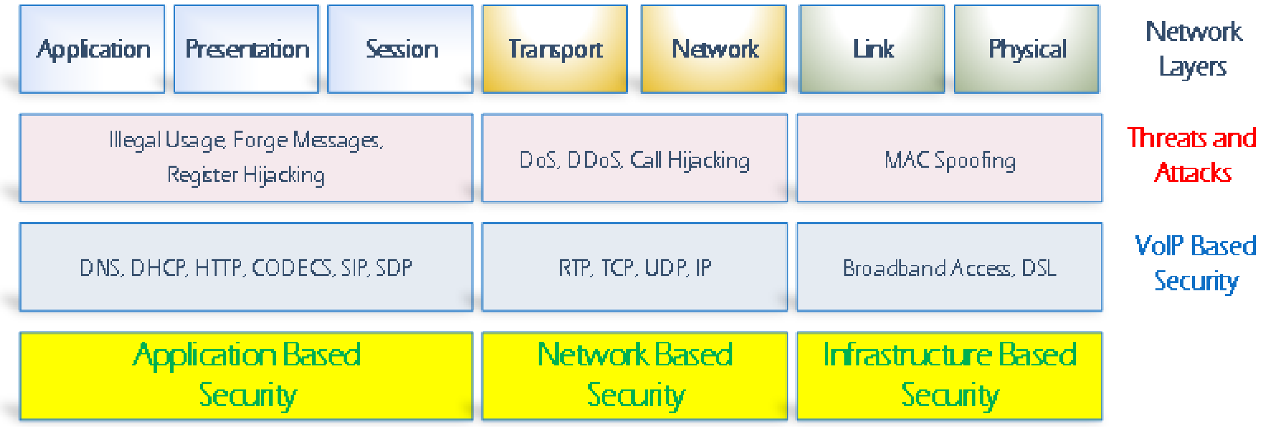
Figure 7.1: Stack of VoIP Protocols and Security Layer.

As per my research, VoIP security general requirements such as …

1. Just deal with the server that have a valid digital certificate.
2. Proper user authentication using proxy and identity server with source IP address.
3. Phone no must be translated into IP address before communication.
4. Identify location of gateway to track caller IP address.
5. Use Caller ID encoding and decoding while calling.

6. Call details record must be maintain.

Above are general security measures that we have to follow but layer based security such as…



Application	Presentation	Session	Transport	Network	Link	Physical	Network Layers
Illegal Usage, Forge Messages, Register Hijacking			DoS, DDoS, Call Hijacking		MAC Spoofing		Threats and Attacks
DNS, DHCP, HTTP, CODECS, SIP, SDP			RTP, TCP, UDP, IP		Broadband Access, DSL		VoIP Based Security
Application Based Security			Network Based Security		Infrastructure Based Security		

Figure 7.2: Layer Based Security for VoIP.

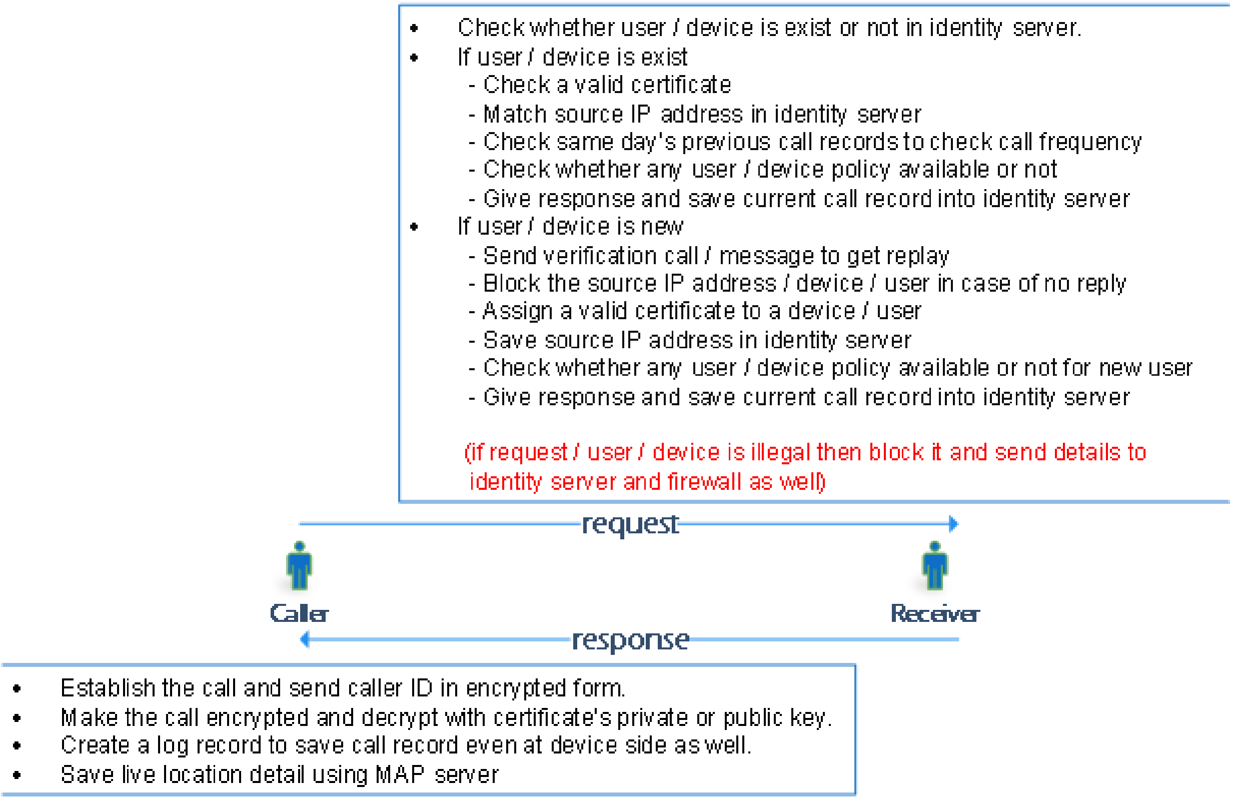
Security Steps as per Network Diagram

1. Unnecessary services must be turned off.
2. VoIP server access must be restricted.
3. Use IDS to detect illegal attempt of VoIP server.
4. VoIP firewall must be used.
5. User identity must be confirmed and cross checked using Proxy and Identity Servers.
6. Keep call records or message records for future auditing.
7. Use certificate servers to authenticate user and devices.
8. Use encryption of call and messages.
9. Implement MapPoint Server to track users.
10. Certificate server must be in all VoIP network to identify users and devices.

Network Diagram:

Figure 7.3: Network Design for Secure VoIP.

Protocol



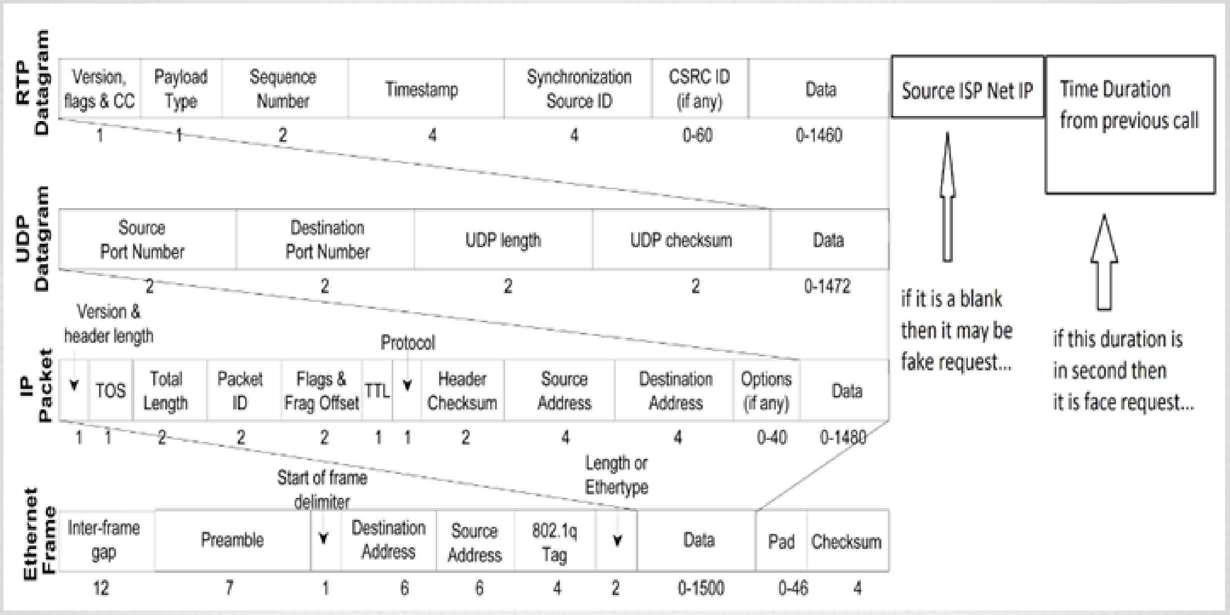
- Check whether user / device is exist or not in identity server.
- If user / device is exist
  - Check a valid certificate
  - Match source IP address in identity server
  - Check same day's previous call records to check call frequency
  - Check whether any user / device policy available or not
  - Give response and save current call record into identity server
- If user / device is new
  - Send verification call / message to get replay
  - Block the source IP address / device / user in case of no reply
  - Assign a valid certificate to a device / user
  - Save source IP address in identity server
  - Check whether any user / device policy available or not for new user
  - Give response and save current call record into identity server

(if request / user / device is illegal then block it and send details to identity server and firewall as well)

- Establish the call and send caller ID in encrypted form.
- Make the call encrypted and decrypt with certificate's private or public key.
- Create a log record to save call record even at device side as well.
- Save live location detail using MAP server

Figure 7.4: Protocol.

We need to add these two fields for secure VoIP:



RTP Datagram	Version, flags & CC	Payload Type	Sequence Number	Timestamp	Synchronization Source ID	CSRC ID (if any)	Data
	1	1	2	4	4	0-60	0-1460

UDP Datagram	Source Port Number	Destination Port Number	UDP length	UDP checksum	Data
	2	2	2	2	0-1472

IP Packet	Version & header length	TOS	Total Length	Packet ID	Flags & Frag Offset	TTL	Protocol	Header Checksum	Source Address	Destination Address	Options (if any)	Data
	1	1	2	2	2	1	1	2	4	4	0-40	0-1480

Ethernet Frame	Inter-frame gap	Preamble	Start of frame delimiter	Destination Address	Source Address	802.1q Tag	Length or Ethertype	Data	Pad	Checksum
	12	7	1	6	6	4	2	0-1500	0-46	4

Source ISP Net IP	Time Duration from previous call

if it is a blank then it may be fake request...

if this duration is in second then it is face request...

Figure 7.5: These two fields can help trace & secure.

Check should be performed on Source ISP as shown in below diagram:

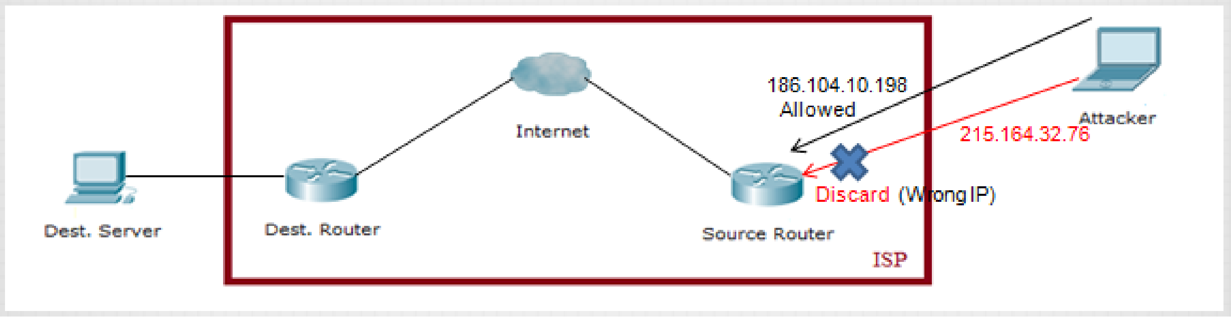


Figure 7.6: Check on Source IP.

Chapter 8

Conclusion and Future Scope

8.1 Conclusion

In the world there are a lot of theories regarding VoIP securities and services. But VoIP is actually more secure and reliable than normal internet based services such as email, chat, voice mail, fax and etc. And we need not to worry about security because security is being implemented day by day. Now days VoIP is more secure than its beginning days. But still we need to be very careful while sending sensitive information using VoIP.

VoIP security issues are challenging task for networking staff and with this technology, added threats, warms and others issues are being shown but stiff it is safe because of efficient network and protocol design as we did in this research.

An individual who manage VoIP based networks have a endless job. In large organizations, the security and network are divided into different groups to manage in a proper way.

8.2 Future Scope

In RAN's

Bibliography

[1] Dennis Hartmann and Josh Finke, "Cisco Unified Communications Manager Architecture," in Implementing Cisco Unified Communications Manager, 2nd edition, Cisco Press, 2012.

[2] VoIP v/s PSTN Connections Graph,
http://www.ce-mag.com/archive/1999/marchapril/Shergold.html

[3] Introduction, http://www.rdegges.com/transparent-telephony-part-1-an-introduction/.

[4] PSTN, http://www2.uic.edu/stud_orgs/prof/pesc/part_1_rev_F.pdf

[5] ISDN, http://netcert.tripod.com/ccna/wan/isdn.html

[6] Unified Networks, http://www.networkworld.com/newsletters/2008/0225msg1.html

[7] Unified Networks, http://www.ipanematech.com/en/take-advantage-of-dynamic-hybrid-networking

[8] RAN,
http://wwwen.zte.com.cn/endata/magazine/ztetechnologies/2009year/no3/articles/200903/t20090312_170857.html

[9] FoIP, http://home.howstuffworks.com/foip.htm

[10] CoIP, http://searchunifiedcommunications.techtarget.com/definition/CoIP.

[11] VoIP Introduction, http://www.tucker-usa.com/voip/voipabout.html.

[12] VoIP Introduction, http://www.cisco.com/en/US/prod/voicesw/networking_solutions_products_genericcontent0900aecd804f00ce.html

[13] VoIP, http://www.voipmechanic.com/what-is-voip.htm.

[14] VoIP Protocols, http://www.protocols.com/pbook/voipfamily.htm.