Secured VoIP application: Final Report

Arnav Dutta

[Bhumika Saivamani](https://www.facebook.com/bhumika.saivamani?fref=grp_mmbr_list)

[Rajen Patel](https://www.facebook.com/rajenpatel91?fref=grp_mmbr_list)   
Swetalina Behera

**Table of Contents:**

Contents

[**Overview:** 3](#_Toc386737936)

[**Introduction:** 3](#_Toc386737937)

[**Available VoIP and problem:** 4](#_Toc386737938)

**Our VoIP**:………………………………………………………………………………………………………………………………………………..5

[**Features of our application:** 7](#_Toc386737939)

[**Challenges faced:** 9](#_Toc386737940)

[**Conclusion:** 9](#_Toc386737941)

[**References:** 9](#_Toc386737942)

# **Overview:**

The purpose of this document is to describe in detail the final design and implementation of our Network Security Project 6349: To develop a secured VoIP Application which will use SIP for signaling and RTP for media (voice) exchanges and trying to implement as many security features available over it.

# **Introduction:**

**Voice over Internet Protocol** (**VoIP**):

Voice over Internet Protocol (also called VoIP, IP telephony, Internet telephony and Digital Phone) is the routing of voice conversation over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of traditional dedicated circuit-switched voice transmission lines.

Advantages of VoIP include toll bypass, network consolidation and service convergence. Thousands of dollars are saved for large enterprises by placing long distance calls over an IP network instead of traditional telephone system. Network consolidation enables the transmission of data, voice, and video over one single network. The integration greatly reduces setup and maintenance costs. With service convergence, enhanced functionality can be implemented through coupling of multimedia services. The deployment rate of VoIP is increasing steadily.

**SIP:**

SIP, the session initiation protocol, is the [IETF](http://www.voip-info.org/wiki/view/IETF) protocol for VOIP and other text and multimedia sessions, like instant messaging, video, online games and other services.

SIP is very much like HTTP, the Web protocol, or SMTP. Messages consist of headers and a message body.

* SIP is a text-based protocol that uses UTF-8 encoding
* SIP uses port 5060 both for UDP and TCP. SIP may use other transports

SIP offers all potentialities of the common Internet Telephony features like:

* call or media transfer
* call conference
* call hold

Since SIP is a flexible protocol, it is possible to add more features and keep downward interoperability.

**RTP:**

The **Real-time Transport Protocol** (**RTP**) defines a standardized packet format for delivering audio and video over IP networks. RTP is a standard specified in RFC 1889. RTP gives no guarantee for timely delivery but provides suitable functionality for carrying real-time content, e.g., a timestamp and control mechanisms for synchronizing different streams with timing properties. RTP is basically a combination of two parts -

* Real Time Protocol (RTP): It carries real-time data.
* Real Time Control Protocol (RTCP): It monitors the quality of service and conveys information about the participants.

# **Available VoIP and problem:**

Securing VoIP system is more challenging than securing pure data network. First, all security problems related with data network appear in VoIP system since they share same network infrastructure. Secondly, VoIP does not have a dominant standard so far. The support of two standards in products just increases the chance of buggy application. Dozens of proprietary protocols make the matter worse. Thirdly, the QoS (Quality of Service) requirement of VoIP leaves less working room for possible security measures. A very secure VoIP system that cannot deliver good voice quality is not attractive.

Some existing VoIP systems with security deficiencies:

* Twinkle: supports SRTP and ZRTP but doesn’t have TLS.
* X-Lite: no security features implemented.

**Problems present in our Server which we tried to address:**

1. Using sniffing tools like Wire shark we can capture the audio call. So there is a strong need to implement SRTP.

2. Authentication Process of SIP while registering the client and server can be compromised by observing the response messages through sniffer tools like wireshark.Attacker can import hashlib and generate hash values with the available information and by using Brute force can guess the password.

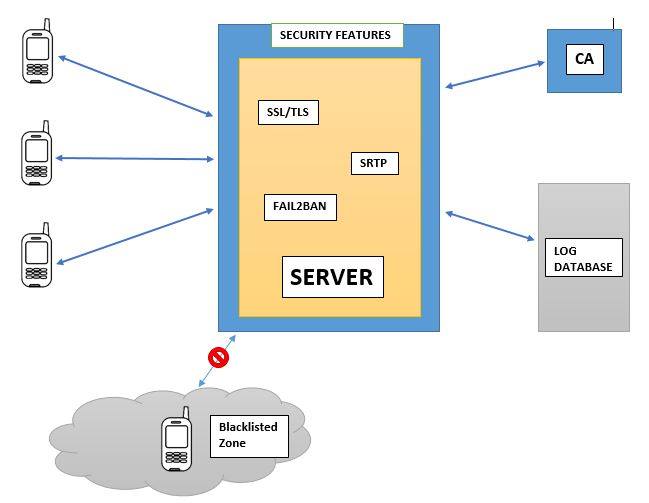
3. SSL/TLS is not implemented in certain VoIP Clients. And hence Integrity is not achieved and the systems are prone to Meet in middle attacks. To improvise that, SSL/TLS functionality is included in our proposed VoIP system.

4.  Blacklist Functionality includes rejecting or ignoring calls/any other type of communication from particular entity or Domain.This functionality plays a major role when we want to avoid making communication with particular country.

5. Generally Servers generate log.But they remain innon readable format.Logs can be used to determine characteristic of various users particularly attackers/hackers if we want to know behavior of attacker.

**Our VOIP:**

**ARCHITECTURE OF OUR SYSTEM**



**Components of the System:**

**1.Server:** Configuration of Asterisk is accomplished through a variety of ‘.conf’ files. The modifications we have made to these are given below.

* + **Sip.conf :**
    - In this file context is created and SIP Users are Listed.Along with the SIP Name and Passwords.
  + **Extensions.conf**
    - In this file for each context in sip.conf,extension statements are defined.Like for call,message,voicemail etc.
    - Priority to those functionalities are defined.
  + Fail2Ban is used.
    - It is an intrusion detection/prevention system. It works by scanning log files and then taking action based on the entries in those logs.
    - Fail2Ban is implemented with a configuration to be able to prevent SIP brute force attacks against our Asterisk.
    - It protects system against brute force attacks.

**2.Client:**

* For implementing client in our project we are using various available android/linux sip clients.
* We ran our project on following clients:
  + **Zoiper**: ZOIPER Free Edition V.2.0 has many features to provide you with a very comfortable calling experience:
  + **Blink**: Blink client provides real-time communications including audio, chat, presence, file transfer and screen sharing using SIP protocol.
  + **Jitsi:** Open Source SIP Communicator with facilities to use encryption protocols SRTP/ZRTP.It has many features like Auto answer and auto forward,call recording,conference calls,IPv6 support for SIP,Encryption password storage using a Master Password.Since it is written i Java ,Easy to modify the code.
* **3.Certificate authority:**
* Self Signed Certificates are created and used to provide authentication,confidentiality services.
  + Steps:
    - Server generates self signed certificate.
    - Generate client certificate
    - Add code for TLS connection configuration in sip.conf file
    - Server will distribute the certificate to the client via email.
    - Client configures the certificate and uses it.

**4.Log Database:**

Log database stores the activities of user in the log. It includes how many times the user has logged in, when and from where the user has logged in and so on.Through logs certain rules can be written and behavior of attackers profile can be identified.

# 

# **Features of our application:**

**1.Call**:

To establish a call between Clients.

* The following steps are done.
  1. Changes in sip.conf:
     1. Under general category, Set the general settings like Local Ip,Bind address,Bind Port,default context
     2. Create users who can register with the server.
     3. For every user set the type of user,host type,password to access the server and context specific to the user.
  2. Changes in extensions.conf:
     1. Under each context define extensions and their properties,along with priority for those properties.
     2. Functions like Answer,Dial,Playback,Voicemail,Hangup are available.

**Configuration Files :sip.conf,extensions.conf**

**2.SMS**:

For implementing SMS feature in our application we did following modifications:

a.In sip.conf file:

i.Parameters set to accept out of call messages.

ii.Then context is defined for that.

b.In the extensions.conf,

i.MessageSend,NoOp,Hangup functions are defined.

**Configuration Files : sip\_sms.conf,Extensions\_sms.conf**

**3.TLS/SSL**

Asterisk has **ast\_tls\_cert** script to create self signed certificate and asterisk certificate.User is prompted to enter the passphrase. CA certificate and asterisk certificate in pem format is generated.Everytime user needs to confirm the passphrase.

Then Server sends the certificate to client through email.And the client configures the certificate.

Add the following code to enable TLS/SSL parameters in **sip.conf:**

|  |
| --- |
| tlsenable=yes  tlsbindaddr=0.0.0.0  tlscertfile=/etc/asterisk/keys/asterisk.pem  tlscafile=/etc/asterisk/keys/ca.crt  tlscipher=ALL  tlsclientmethod=tlsv1 |

**4. SRTP:**

* Server Side: Enable encryption parameter in sip.conf

|  |
| --- |
| Encryption=yes |

* Client Side: Client should enable SRTP functionality in SSL/TLS compatible client.

**5. Fail2Ban:**

To defend against Brute force attack, Fail2Ban is implemented on top of asterisk server.

**Configuration file: etc/fail2ban/jail.conf**

|  |
| --- |
| [asterisk-iptables]  enabled = true  filter = asterisk  action = iptables-allports[name=ASTERISK, protocol=all]  sendmail-whois[name=ASTERISK, dest=client@mail.com, sender=voip\_project@utdallas.edu]  logpath = /var/log/asterisk/messages  maxretry = 5  bantime = 259200 |

* Maxtry represents the number of times user or client is allowed to try the password.
* If the number of try exceeds maxtry, then log will be stored in the logpath.
* And email is sent to the client mentioned in dest (client).
* This restriction defends against Brute force attack.

**6. Geographical Location Restriction Feature:**

* A shell script is written such that Location restriction is made.
* IP Address of particular countries can be blocked.
* Countries names are added to the Blacklist.
* **Script Name : Country.restrict.iptables.sh**

**7. Log Analysis Intelligence**

* A Configuration file is written.
* It has rules such that it can learn the behavior of the hacker, the entire behavior of users can be obtained by writing efficient rules.
* Example-Rules to read the log and find out how many times wrong password was entered
* Through this way behavior of the hacker can be learn and malicious profile template can be obtained.
* **Configuration File Name : /etc/fail2ban/filter.d/asterisk.conf**

# **Challenges faced:**

1. Working with open source.
2. Selecting and working with android client that supports functionalities like SSL/TLS.
3. Capturing and Analyzing the SIP Packets.
4. Managing the IP tables.
5. Analysis of log behavior.
6. Establish call after implementing SSL/TLS.

**Contributions:**

[Rajen Patel](https://www.facebook.com/rajenpatel91?fref=grp_mmbr_list) :

Build sever, VoIP vulnerability analysis using Wireshark sniffers, Prevention Against brute-force (fail2ban), Geographic location restriction (black list implementation), Heuristic rule added

Arnav Dutta: Establish call, Implemented SRTP

[Bhumika Saivamani](https://www.facebook.com/bhumika.saivamani?fref=grp_mmbr_list): SMS and SSL/TLS and log analysis

Swetalina Behera: SMS and SSL/TLS and log analysis

# **Conclusion:**

We addressed current security breaches like brute force attack. Addition to it, we have added SRTP, SSL/TLS, Geographical location restriction and log intelligence. These security features make VoIP more reliable and secure.

# **References:**

1) [www.**asterisk**.org/sites/**asterisk**/.../**asterisk**\_quick\_start\_guide.pdf](http://www.asterisk.org/sites/asterisk/.../asterisk_quick_start_guide.pdf) ‎(asterisk server)

2) www.voip-info.org/wiki/view/**Fail2Ban**+ (with+iptables) +And+Asterisk‎ (Fail2ban tools)

3) [www.gtri.com/improved-**tls**-**ssl**-security-with-dane/](http://www.gtri.com/improved-tls-ssl-security-with-dane/) (TLS/SSL)