

# SECURING VOIP COMMUNICATIONS IN AN OPEN NETWORK

Mukund Sarma<sup>1</sup>

<sup>1</sup>Dept. of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, Amrita School of Engineering, Amritanagar, Coimbatore, India, 641112.

## Abstract

Channeling voice calls over IP networks has brought many advantages to enterprise communications, but it also creates some security risks. In this paper a technique to enhance the security of vocal and text communication is proposed. This technique is a combination of multipath routing and secret sharing scheme. Information is conveyed securely from one person to another over an open network using the secret sharing scheme. The original data is divided into two shares and each of these shares is sent over the open network through multiple different paths using the multipath routing technique. In case of a man-in-the-middle attack the person will not obtain any information of the original form with only one of the shares. Only if the person collects both the shares he/she can reconstruct the original information. A mechanism to secure SIP (Session Initiation Protocol) and text communication is also discussed in this paper.

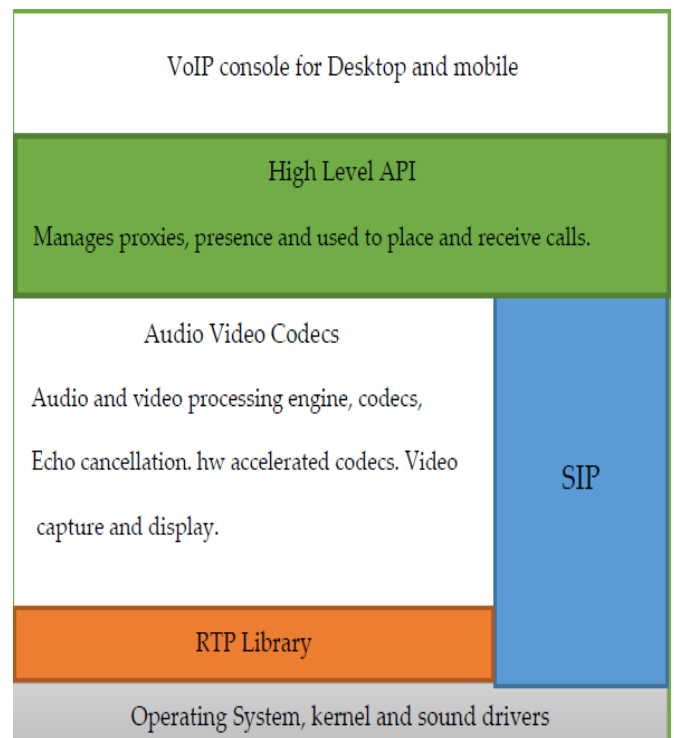
**Keywords:** VoIP, Secret sharing scheme, Multipath routing, Speech compression, RTP, TLS, SIP.

\*\*\*

## 1. INTRODUCTION

In the early days of VoIP, there was no big concern about security issues related to its use. People were mostly concerned with its cost, functionality and reliability. Now that VoIP is gaining wide acceptance and becoming one of the mainstream communication technologies, security has become a major issue. There are many security concerns in VoIP such as denial of service, alternation of voice stream, eavesdropping, redirection of call, data manipulation, caller ID imitation and man in the middle attacks.[1][2] To understand these concerns and know how handle them, the architecture of VoIP needs to be understood clearly. In the public switched telephone networks (PSTN) the entire communication paths were administered by officials. So the risk of man-in-the-middle attack is not as high as in the case of VoIP which has multiple intermediate exits between the two users.

As a developer, to understand what the security risks in VoIP are, he/she needs to understand the architecture and working of VoIP. Figure 1 depicts the software architecture of VoIP. This architecture is similar to that of Linphone's software architecture. [15]

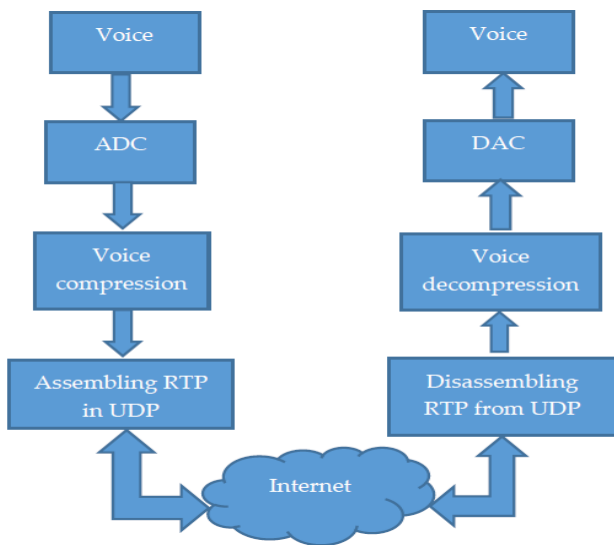


**Fig 1** Software architecture of VoIP

Working of VoIP: The caller starts to speak once a call has been set up between two, or more, VoIP devices. At this point the voice signal is converted into a digital signal, formatted for transmission and sent along the network to the destination, where all of the preceding steps have to be reversed.[3] Figure 2 describes the architecture diagram of how VoIP works.

**Steps:**

1. First the ADC converts analog voice to digital signals (bits)
2. Now the bits are compressed in a format which is best for transmission
3. The payload (voice packets) are inserted in data packets using a real-time protocol (typically RTP over UDP over IP)
4. A signaling protocol is needed to call users: SIP (Session-initiation protocol) does that.
5. At the other end packets are disassembled, data is extracted and then they converted to analog voice signals and sent to the phone.
6. Quality of Service (QoS) makes sure all this happens in the real time as one cannot wait for too long for a reply.



**Fig 2** Working of VoIP

While circuit switching keeps the connection open and constant, packet switching opens a brief connection long enough to send a packet, from one system to another. The sending device (computer/phone) opens a port/channel and sends the packet. . The risk of man-in-the-middle attack is high in the case of VoIP which has multiple intermediate exits between the two users.

Man-in-the-middle attacks, eavesdropping and data manipulation can happen as voice traffic travels over the Internet. It is relatively easy for someone to eavesdrop on the media stream and obtain data. In order to prevent eavesdropping, a set of security protocols, called IPsec, is used to apply encryption to the digitized voice stream for VoIP. But this again involves key exchange and is vulnerable to man-in-the-middle attacks.

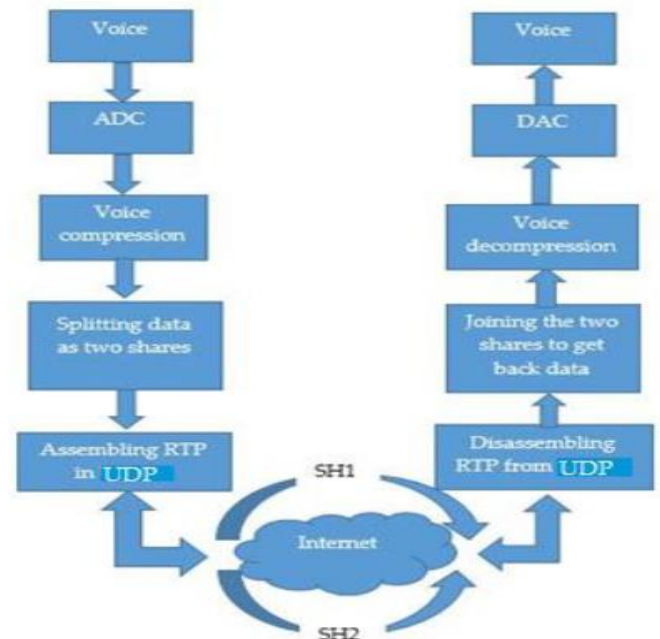
Caller ID manipulation, redirection of a call, hijacking the session by registering happens when an attacker postures as a valid VoIP user and then hack into the system. Hijacking is possible because the signaling messages that the SIP sends as

plain text with no guarantee that the data that is received at the receivers end is indeed the data sent by the user.

**2. SECURING VOICE CALLS IN THE PROPOSED METHOD**

Voice is first converted from analog to digital (bits) using an ADC (Analog to Digital Converter). The steps involved in digitizing voice include sampling, quantizing, silent suppression and compression. Since it is a vocal call, even if there is a small loss in data it won't affect the conversation. So a lossy compression minimizes the amount of data that needs to be transmitted. Codecs such as opus, SILK, speex, PCMU, iSAC etc. can be used for compression of data. [4][5] The SIP server chooses which type of codec is to be used for the call.

The compressed data is cut into a constant size of 256 bits. This 256 bit alphanumeric string is then divided into two equal strings. These two 128 bit strings are converted into images. Visual cryptography is applied on these two images and these are now called shares. These shares are then sent on the open network using the concept of multipath routing. At the other end these shares are joined together and decrypted to get the message back in its original form. The use of visual sharing scheme eliminates the risk of eavesdropping. Another advantage of using the shares is that it does not require any key exchange. Since both the shares are sent on two random ports, even if there is a man-in-the-middle-attack he will not be able to modify the data. Figure 3 describes the working of the proposed method. [6]



**Fig 3** Working of the proposed method SH1 and SH2 are shares 1, 2 respectively.

**Working of Shamir’s Visual Sharing Scheme:**

Visual secret sharing schemes (VSS) represents the particular case of secret sharing scheme where the shares are images. Naor and Shamir were the first to introduce them as a part of visual cryptography [7] [8] [9]. Each image (share) is considered to be a matrix of pixels. By convention, in black-and-white representation, a white pixel is represented by 0 and a black pixel is represented by 1.

Example of Naor-Shamir VSS for two participants or two devices

$$S^0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}; S^1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Corresponding shares in Shamir’s VSS with 2 participants in the pixel notation are shown in Table 1. [10]

**Table 1** All possible shares in Shamir’s VSS with 2 participants















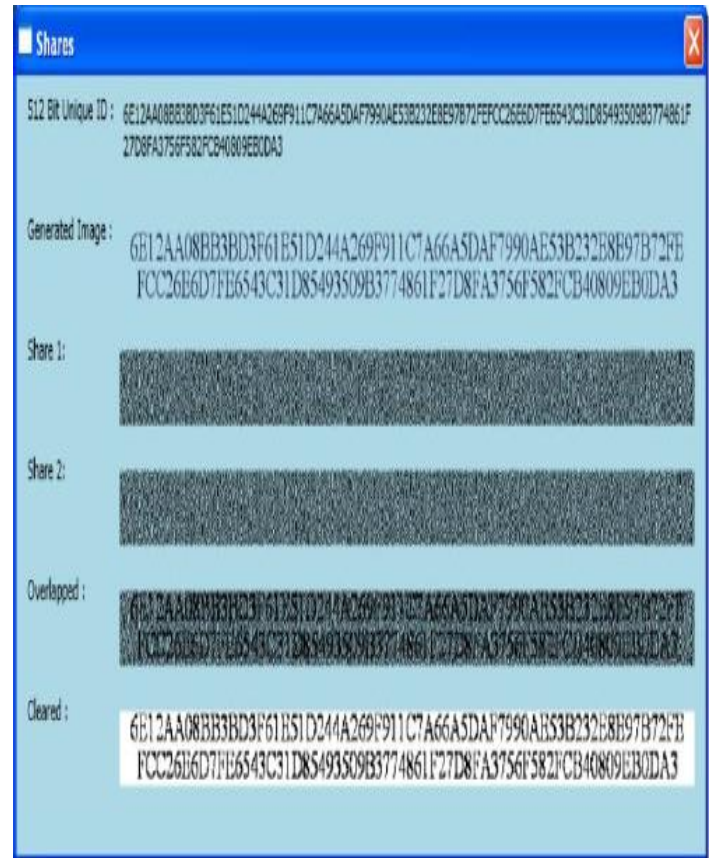
White Pixel  	1 <sup>st</sup> Share		
	2 <sup>nd</sup> share		
	Result		
Black Pixel  	1 <sup>st</sup> Share		
	2 <sup>nd</sup> Share		
	Result		

Figure 4 shows how the digitized 512 bit number is converted to shares and how the two shares are overlapped to get back the original data.



**Fig 4** Shares of a 512 bit digitized string

**Multipath Routing:**

Multipath routing is a technique that allows data to be sent over multiple alternate paths. This is in contrast to a single routing protocol, where a data stream is directed along a single path from a source to a destination. With multiple paths, the source and destination pair can use any number of alternate routes to achieve performance enhancements, connection stability, and potential security improvements. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines.

The data (share) is secure when communications are distributed across multiple paths. Here, instead of an intruder observing a common route, as in the case of single path routing, the data is spread out among alternate routes. This makes it difficult for an attacker to determine all the possible routes for a communication and thereby limit his/her interception of the data to a very small volume if one of the routes is being observed. Several methods have been studied in finding out disjoint paths. The concept of disjoint multipath routing is used to send packets for a particular session. [11] [12]

### 3. SECURING TEXT COMMUNICATIONS IN THE PROPOSED METHOD

VoIP applications make use of SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) an instant messaging and presence protocol suite based on Session Initiation Protocol (SIP). SIP is a signaling protocol, used for controlling multimedia communication sessions such as voice and video calls over the Internet. The protocol governs establishment, termination and other essential elements of a call.

Messages sent are in the form of Plain text. Any intruder will be able to find out the user name, password and the data. The authentication (The users identity), Integrity (Is the message received the same as the one sent?), privacy and confidentiality (Is someone listening to the conversation?) are at stake. [13]

One way to go about securing SIP is using TLS (Transport Layer Security) in SIP [14]. The other way is to encrypt the messages being sent and received to and from the SIP server. An application is developed at the server side that decrypts the encrypted messages that are being sent from the VoIP devices.

If the SIP is not secured, there is a risk of attackers making unauthorized calls and gaining access to the VoIP network. This could lead to the access of private conversations made on the VoIP network thereby modifying the messages if needed or bringing down the entire VoIP network. [13]

TLS provides an encrypted channel that can be used to send SIP messages. A public key cryptography algorithm is used to encrypt the messages.

### 4. SUMMARY

The proposed method aims to reduce the security risks involved in VoIP communication. Security risks involving voice communication is reduced using the concept of visual cryptography and multipath routing technique. The Shamir's visual sharing scheme has been implemented to achieve the secret sharing scheme. The shares generated are then sent over the network using the concept of disjoint multipath routing. The paper also proposes two methods on how to secure text communications in VoIP. The proposed method ensures the security concerns in VoIP such as denial of service, alternation of voice stream, eavesdropping, redirection of call, data manipulation, caller ID imitation and man in the middle attacks are not compromised.

### ACKNOWLEDGMENTS

I am highly indebted to Amrita Vishwa Vidyapeetham for their kind co-operation and encouragement which help me in doing this project. I also wish to express sincere gratitude to ADRIN, Department of Space, Government of India for

providing me necessary guidance and support required to work on this project.

### REFERENCES

- [1]. Hung P.C.K., Martin M.V. 2006."Security Issues in VOIP Applications" Electrical and Computer Engineering Conference (CCECE).ISBN:1-4244-0038-4. pp: 2361-2364. DOI:10.1109/CCECE2006.2777789
- [2]. D. Butcher, X. Li, and J. Guo, 2007. Security Challenge and Defense in VoIP Infrastructures, IEEE Trans.Systems, Man, and Cybernetics Part C: Applications and Reviews, vol. 37, no. 6, pp. 1152–1162
- [3]. Khaled Salah, "On the Deployment of VoIP in Ethernet Networks: Methodology and Case Study", Department of Information and Computer Science, King Fahd University of Petroleum and Minerals. <http://faculty.kfupm.edu.sa/ics/salah/voiptool/papers/ComCom m.pdf>
- [4]. Malik Ahsan Ali, Imran Rashid, Adnan Ahmed Khan, 2013. "Selection of VoIP CODECs for Different Networks based on QoS Analysis". International Journal of Computer Applications (IJCA), Vol 84 Issue 5, DOI: 10.5120/14575-2702
- [5]. Leigh A. Thorpe, 1999. "Subjective evaluation of speech compression codecs and other non-linear voice-path devices for telephony applications", International Journal of Speech Technology. vol. 2, pp: 273-288. DOI: 10.1007/BF02108644
- [6]. Ryouichi Nishimura, Shun-ichiro Abe, Norihiro Fujita and Yoiti Suzuki, Nobuyuki Enomoto, Tsutomu Kitamura and Atsushi Iwata, 2010 "Reinforcement of VoIP Security with Multipath Routing and Secret Sharing Scheme "Journal of Information Hiding and Multimedia Signal Processing. ISSN 2073-4212. Ubiquitous International Volume 1, Number 3, pp: 204-219.
- [7]. Moni Naor, Adi Shamir, 1995. "Visual Cryptography", Advanced in Cryptology – EUROCRYPT'94, LNCS950. Springer-Verlag. pp: 1-12.
- [8]. C. Blundo, S. Cimato, and A. De Santis, 2006. "Visual Cryptography Schemes with Optimal Pixel Expansion", Theoretical Computer Science, vol 369, pp: 169–182.
- [9]. C. Blundo, A. De Santis, D.R. Stinson, 1999. "On the contrast in visual cryptography schemes", J. Cryptology, vol 12, pp: 261–289.
- [10]. Ruxandra Olimid, "Python Implementation of Visual Secret Sharing Schemes", Journal of Information Systems & Operations Management, Vol.5.2.1.
- [11]. S.-J. Lee and M. Gerla, 2001. "Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks", Proc. of Int. Conf. on Communications, vol. 10, pp: 3201-3205.
- [12]. W. Lou and Y. Fang, 2001. "A Multipath Routing Approach for Secure Data Delivery", Proc. of Military Communications Conference (MILCOM), vol. 2, pp: 1467–1473

- [13]. Salsano S, Veltri L, Papalilo D, 2002. "SIP security issues: the SIP authentication procedure and its processing load" *Network*, IEEE, Vol 16, issue 6, pp: 38-44, DOI: 10.1109/MNET.2002.1081764
- [14]. Tadashi Kaji, Kazuyoshi Hoshino, Takahiro Fujishiro, Osamu Takata, Akifumi Yato, Keisuke Takeuchi, Satoru Tezuka, 2006. " TLS handshake method based on SIP", *Proceedings of the International Multiconference on Computer Science and Information Technology*, pp: 467 – 475
- [15]. *Software Architecture* (2014) Available at: <http://www.linphone.org/eng/documentation/dev/> (Accessed: 8 Febuary 2014)