International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

Secure VoIP Transmission through VPN Utilization

Prashant Khobragade
Department of Computer Science & Engineering
RGCER
Nagpur, India
prashukhobragade@gmail.com

Disha Gupta
Department of Computer Science & Engineering
RGCER
Nagpur, India
disha.g14@gmail.com

Abstract **—**Voice over IP (VoIP) is one of the rapidly growing communication technologies. However, the widely used VoIP protocol suite, H.323 is unable to maintain its performance when it is concerned with scalability. To overcome these limitations and to manage and establish multimedia sessions Session Initiation Protocol (SIP), a lightweight application layer protocol was designed. But being a text-based protocol it has high vulnerability to security attacks. Thus to provide users with a secure communication platform methods are required to pursue protection for SIP VoIP system. At the same time QoS is also to be maintained to assure service's performance and to avoid degradation of speech quality. Thus, the proposed approach is based on virtual private network (VPN) tunneling utilization for securing communication on VoIP network while maintaining the quality.

Index Terms**—**Voice over IP (VoIP), H.323, Session Initiation Protocol (SIP), Virtual Private Network (VPN).

I. INTRODUCTION

As a result of the rapid technological advancement, long distance communication has become a common need and thus one of the important aspects of human lives. Telecommunication has been proved as a great medium for the distant educational resources, business promotion, voice communication and entertainment. Besides its large impact on economic market, it has also lead to social closeness among the people from all over the world.

The development of special-purpose switching chips, coupled with highly reliable fiber-optic transmission systems, has made it possible to build economical, ubiquitous, high-speed packet-based data networks. Similarly, the development of very fast, inexpensive digital signal processors (DSPs) has made it practical to digitize and compress voice and fax signals into data packets. The natural evolution of these two developments is to combine digitized voice and fax packets with packet data, creating integrated data-voice networks.

Voice over Internet Protocol (VoIP) is a rapidly emerging technology for voice communication that uses the ubiquity of IP-based networks to deploy VoIP-enabled devices in enterprise and home environments. A VoIP application encodes, transmits and decodes voice signals over the internet

in the form of packets. As only one network is used to deal with two kinds of streams instead of using traditional separate data and voice networks, much more cost reduction can be achieved on the service [1]. The VoIP networks replace the traditional public-switched telephone networks (PSTNs), as these can perform the same functions, with more convenience and ability to reduce call expenses.

Fig.1. Basic VoIP Environment

These functions generally include signaling, data basing, call connect-disconnect, and coding-decoding. A brief description of these functions is given as follows:

I. *Signaling:* Signaling in a VoIP network is accomplished by the exchange of IP datagram messages between the components. The format of these messages is covered by the standard data link layer protocols.

II. *Database services:* Database services are a way to locate an endpoint and translate the addressing that two networks use; for example, the PSTN uses phone numbers to identify endpoints, while a VoIP network could use an IP address and port numbers to identify an endpoint. A call control database contains these mappings and translations.

III. *Calls connect-disconnect (bearer control):* The connection of a call is made by two endpoints opening communication sessions between each other. In the PSTN, the public (or private) switch connects logical channels through the network to complete the calls. In a VoIP implementation, a multimedia stream (audio, video, or both) is transported in real time. The connection path is the bearer channel and represents the voice or video content being delivered. When communication is complete, the IP sessions are released and, optionally, network resources are freed.

IV. *CODEC operations:* Voice communication is analogue, while data networking is digital. Analogue waveforms are converted into digital information by using a coder-decoder (CODEC).

While performing these operations VoIP faces two major challenges which are found to be more serious as compared to the traditional PSTN networks. These challenges are maintenance of quality of service and security. Due to extent of infrastructure sharing present in VoIP networks, it does not guarantee similar quality as in PSTN network.

Its service quality consists of the following factors: Network Availability, Latency, Jitter and Packet Loss [2]. Since VoIP is an application in information-technology oriented network, damages such as theft of data, privacy breach, loss of time, disabled or crippled service can be probably caused by the vast interconnection which contributed

to the advantage of Internet too [3]. Thus, balancing between QoS and security is important to SIP application [4] in VoIP.

This paper is organized as follows: Section II describes the background work. A provision for securing the VoIP server through VPN tunneling is proposed in Section III. Finally, Section IV concludes the paper and discusses the future scope.

V.BACKGROUND WORK

VI. VoIP Protocol Stack

VoIP technology employs a suite of protocols which can be categorized into signaling and data transfer protocols. The following figure [5] shows the essential protocols in a typical VoIP protocol stack.

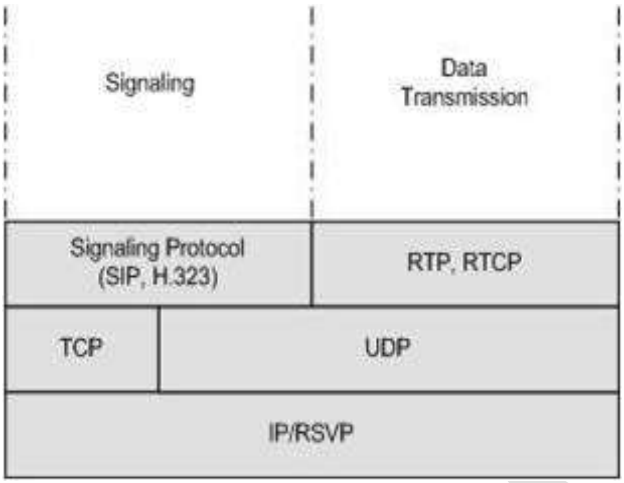

Fig.2. Essential protocols in a VoIP protocol stack

The signaling protocols are in charge of setting up, managing, controlling and terminating a session. The voice transmission protocols are responsible for transmitting the actual voice data across the network.

VII. Signaling Protocols

Both H.323 and SIP provide functionalities for call setup, management, and termination. These protocols enable negotiation of the codec to be used in voice data encoding and the delivery mechanisms (e.g. RTP [6] over UDP/IP [7]) for both protocols.

1) H.323

H.323 is a protocol suite that was designed to enable IP-based multimedia communications, and it was the first widely adopted and deployed VoIP protocol. H.323 protocol suite is shown in figure [8] below:

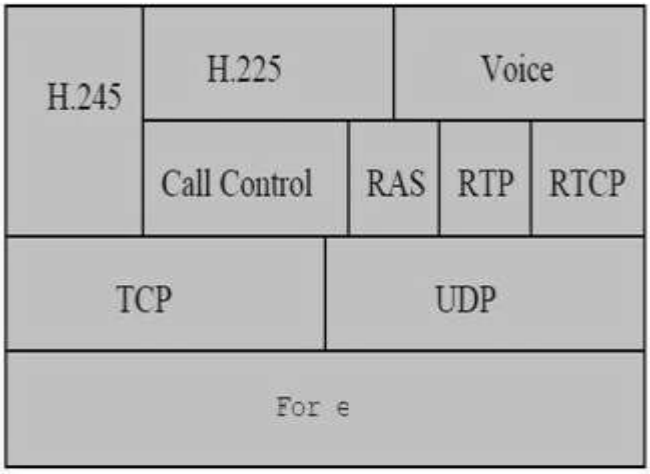

Fig.3. H.323 Protocol Suite

The core protocols contained in H.323 suite are:

- H.245 for opening and closing logic channels for each multimedia session. It is also in charge of capacity and codec negotiation. Two H.323 end points can set up a fast connection without a gatekeeper, by exchanging H.245 messages.
- H.225 for call setup, alert, connecting, and call termination.
- RAS (Registration, Admission, Status) is used to phone management. It establishes logical channels between phones and gatekeepers that manage these phones. Without appropriate RAS communication, a phone cannot place or receive phone calls.
- RTP is used for sending or receiving multimedia information.

While H.323 is the most widely used VoIP protocol suite, it has a number of drawbacks. Although it was originally designed to be used on a LAN, but when there are multiple domains, H.323 has a scalability problem as there is no easy way to perform loop

detection. The complexity which stems from the use of several protocol components, is another drawback. This also complicates firewall traversal. Furthermore, it has poor extensibility, which means it is hard to develop additional extensions for this protocol.

2) Session Initiation Protocol (SIP)

SIP [9] is a lightweight application layer protocol designed to manage and establish multimedia sessions such as video conferencing, voice calls, and data sharing through requests and responses. It is increasingly gaining favor over H.323 in the VoIP environment.

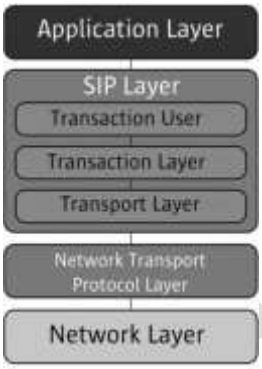

Fig.4. SIP in the Internet Multimedia Protocol Stack

Basic Architecture of SIP:

SIP is used for initiating, modifying, and terminating a two-way interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality [10]. SIP is used in association with its other IETF sister protocols like the SAP, SDP and MGCP (MEGACO) to provide a broader range of VoIP services. The SIP architecture is similar to HTTP (client-server protocol) architecture. It comprises requests that are sent from the SIP user client to the SIP Server. The Server processes the request and responds to the client. A request message, together with the associated response messages makes a SIP transaction.

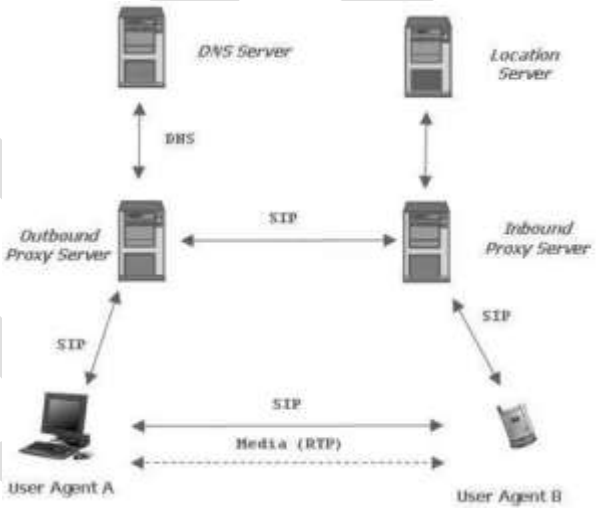

Fig.5. SIP Architecture

SIP is a better candidate for VoIP in terms of simplicity, extensibility and scalability. Since SIP is just an application layer signaling protocol, many security mechanisms are optional and little attention has been given to SIP security features [11]. Compared to its competitor H.323, SIP is more vulnerable on security aspect. This protocol is text-based, which means that there can be some important information, user's encryption for example, encoded into SIP message and unfortunately, these data are usually the goals of attackers to hike or modify. It will be fatal to both users and service provider for privacy breach.

VIII. Virtual Private Network (VPN)

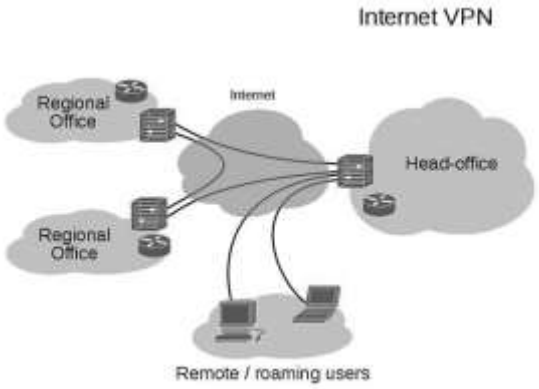

Fig.6. Scenario of a Virtual Private Network

A virtual private network (VPN) extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites but appears to the user as a private network link—hence the name "virtual private network" [12].

IX. VPN Security Model

VPNs typically require remote access to be authenticated and make use of encryption techniques to prevent disclosure of private information. Its security model provides:

- Confidentiality
- Sender authentication
- Message integrity

X. VPN Security Protocols

VPNs provide security through tunneling protocols and security procedures [13] such as encryption. The security protocols include the following:

- IPSec (Internet Protocol Security) was developed by the Internet Engineering Task Force (IETF), for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. Layer 2 Tunneling Protocol frequently runs over IPSec. Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic or secure an individual connection.
- Datagram Transport Layer Security (DTLS) is used to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft's Secure Socket Tunneling Protocol (SSTP) tunnels Point-to- Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- Secure Shell (SSH) offers VPN tunneling to secure remote connections to a network or inter-network links.

XI. PROPOSED WORK

A secure client-server VoIP application can be implemented with two major considerations. First, the integrity of the voice information needs to be preserved; that is, the information must arrive to its destination exactly as it was sent originally. Secondly, the

confidentiality of the voice information needs to be guaranteed. Therefore, voice over IP installations should incorporate effective solutions to both of these security requirements with high performance and balanced Quality of Service (QoS).

Session Initiation Protocol is notoriously difficult to pass through a firewall because it uses random port numbers to establish connections. The proposed system utilizes virtual private network (VPN) tunnels to connect a remote phone to the VoIP Server. It requires that prior placing or receiving phone calls, the VPN connection would need to be up and running.

XII. Architecture for the Proposed Solution

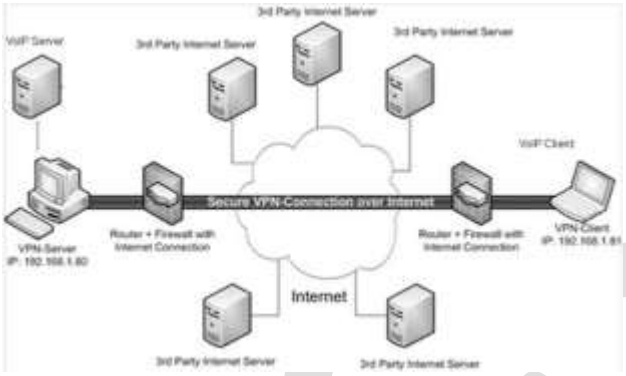

Fig.7. Architecture of proposed VoIP VPN Network

The proposed solution combines VoIP and virtual private network technologies to offer a method for delivering secure voice. Because VoIP transmits digitized voice as a stream of data, the solution accomplishes voice encryption quite simply, applying standard data-encryption mechanisms inherently available in the collection of protocols used to implement a VPN.

XIII. Security Implementation through VPN Tunnel

The basic working of the VoIP application is based on the packet exchange between the VoIP server and VoIP clients who want to communicate. All the VoIP clients send their packets to the VoIP server first which then in turn routes the packet to the destination client. To make this client-server communication secure from VoIP server's point of view, the VPN server establishes tunnel between the client and the server. The VPN server provides security to the VoIP server by encapsulating the digitized voice within IP packets, then encrypting the digitized voice using IPsec, and finally routes the encrypted voice packets securely through a VPN tunnel. At the remote site, another VoIP client decodes the voice and converts the digital voice to an analog signal for delivery to the phone. The same is repeated in reverse order whenever VoIP client sends the packet to the VoIP server.

XIV. Conclusion & Future Scope

VoIP technology is still at the early stage of adoption, and attacks against deployments have been largely unheard of or undetected. As VoIP increases in popularity and numbers of consumers, so does the potential for harm from a cyber attacks. In the proposed solution implementation of VPN tunnel is suggested between the VoIP server and VoIP client. VPN service providers allow flawless communication over the Voice over IP. It provides secured communications between VoIP clients with signaling and media encryption. One of the major features of VPN is no additional configuration and maintenance. This makes it a cost effective security solution for VoIP Server.

Being is a hardware intensive service, sometimes VPN's can take some time to setup, which leads to unnecessary delays. If the strain of encrypting and decrypting traffic on the VPN appliance becomes burdensome, the result may again be delayed VoIP packets and may cause jitter on the VoIP phone. Efficient techniques to resolve above two issues would enable the VPN tunnel to provide enhanced security for VoIP servers in future.

REFERENCES:

[1]. X. Wei, Y. Bouslimani, K.Sellal, "VoIP Based Solution For the Use over A Campus Environment", IEEE - CCECE, 2012

[2]. CCS-WG, "Quality of Service (QoS) Standard for Telephone Services", http://www.ofta.gov.hk/en/ad-comm/tsac/cc-

paper/ccs2005p11.pdf, 2005.

[3]. David Schneider, "The state of network security", Network Security, Volume 2012, Issue 2, 2012.

[4]. X. Wei, K. Sellal and Y. Bouslimani, "Security Implementation for a VoIP Server", International Conference on Computer Science and Service System,2012.

[5]. D. Endler, and M. Collier, "Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions (Hacking Exposed)", McGraw-Hill Osborne Media, 2006.

[6]. H. Schulzrinne, S. Casner, R. Frederick et al., "RFC1889: RTP: A Transport Protocol for Real-Time Applications" Internet RFCs, 1996.

[7]. RFC768, "UDP, User Datagram Protocol, IETF Standard" August, 1980.

[8]. I.Rec,"H.323, Packet based Multimedia Communications Systems, http://www.itu.int/rec/T-REC-H.323/en/," Telecommunication Standardization Sector of ITU.

[9]. RFC 3261, "SIP: Session Initiation Protocol", 2002.

[10]. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. "SIP: Session Initiation Protocol." RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853.

[11]. Mason, Andrew G. Cisco Secure Virtual Private Network. Cisco Press, 2002.

[12]. Walsh, Thomas and Kuhn, Richard, "Challenges in Securing Voice over IP". IEEE Security & Privacy Magazine, Volume 3,Issue 3, May-June 2005, pages 44-49.

[13]. Recommendation ITU-T G.114, "One Way Transmission Time", Int'l Telecomm. Union, 1988.