IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 4 (Nov. - Dec. 2012), PP 24-30
www.iosrjournals.org

Implementing Security on a Voice over Internet Protocol (VoIP) Network: A Practical Approach

Osanaiye Opeyemi Ayokunle
Department of Telecommunication Engineering, Federal University of Technology, Minna, Nigeria.

Abstract: *The internet has been undergoing rapid and continuous growth over the past few years. The most significant development the telecommunication industry has witnessed is the evolution of Voice over IP technology. This technology uses the internet as a medium for transmitting voice during a telephone conversation between two or more parties. VoIP technology comes with numerous benefits like reduced call cost and wide variety of add-ons to both the service providers and the end users. Despite all these, the technology is subjected to security risk because of the open nature of the internet. Much emphasis has been placed on the quality of service of VoIP over the years and dark eyes have been turned on its security.*
This study therefore aims to identify the security threats and attack VoIP can be exposed to during transmission, produce a VoIP system using the open source Asterisks before securing the network using IPSec VPN
Keywords: *VoIP, SIP, H323, QoS, PSTN, VPN tunnel, IPSec, Encryption, Internet, Asterisks*

I. Introduction

Voice over Internet Protocol which is commonly referred to as VoIP is the ability to transmit voice packets in form of telephone calls, faxes or video conferencing over an IP based network. As the internet began to gain popularity through the web in the early eighties, it started to develop into a medium of communication connecting the world together. Among all these development was the evolution of VoIP. VoIP utilizes a common network for both voice and signalling thus enjoying the several advantages it offers like the internet conferencing rooms, personalized call transfer, instant messaging and lots more.

With all its promising attributes and advancement, it has the potential of totally replacing the existing Public Switch Telephony Network (PSTN). Furthermore, the VoIP technology has cheaper call rate, easier IT management and reduction in operational cost for a combined network for voice and data which gives it an edge over the PSTN.

Having mentioned the various promising attributes the VoIP technology posses; its security is often overlooked by voice users. Like any new IT service, VoIP technology has some inherent security risks and vulnerabilities associated with it that can affect the confidentiality, integrity and availability of any organisations IT infrastructure. This security risk is as a result of its architecture which is different from that of the traditional circuit switched based telephone. The aim of this study is to implement security over VoIP network by configuring a VPN (Virtual Private Network) tunnel using IPSec (Internet Protocol Security) that encrypts voice packets over the internet.

II. Voice Over IP (VoIP)

Voice over Internet Protocol (VoIP) which is also referred to as internet telephony is a technology that transmits voice signal in real time using the internet protocol (IP) over a public internet or private data network. [1]. In a simpler term, it converts voice signal which is analogue to a digital signal in your telephone before compressing and encoding it into long strings of IP packets for upward transmission over the IP network to the receiver. At the receiving end, the received IP packets reassembles in order before decompressing and processing through the use of a Digital to Analogue Converter (DAC) to generate the initial signal transmitted [2]. Its existence is basically based on two fundamental technologies, the telephone and the internet.
[3] Identified the sharing of existing infrastructures between both data and voice application as some of the VoIP benefits in reducing implementation, management and support cost.

As this technology began to grow and develop, much emphasis was placed on the quality of service while dark eyes was turn on the security of voice streams being transmitted. The inherent nature of the internet due to its open nature has been a major challenge to the technology with respect to its integrity, confidentiality and availability.

2.1 Voice over IP Architecture

The major goal of the VoIP technology is establishing and managing communication sessions for transmitting both voice and data over a standard IP network. [4], some additional data format like video text or

images may also be supported by VoIP transmission. During this process, a stable and reliable transmission is maintained and the session can be put to end when any of the parties decides to.
According to [5] the two widely used protocols throughout the world today are the H323 and SIP protocol. They are functionally similar but competing protocols from two different organizations. The SIP was developed by the Internet Engineering Task Force (IETF) while the International Telecommunication Union (ITU) developed H323 [6]

2.1.1 Session Initiation Protocol (SIP)

SIP is an application layer protocol specified initially in 1999 by IETF Multiparty Multimedia Session Control Working Group (MMUSIC) and later updated by the SIP WG in 2002 [5]. It is similar to HTTP (Hyper Text Transfer Protocol) as it inherits its message structure used during multimedia session for setting up, cancelling and terminating real time session across an IP network by two or more participants [7]. Some of the benefits it offers include call/session control, extensibility and inherent user mobility [8].
The major driving force behind SIP is to enable VoIP.[9].SIP is currently receiving a wide acceptance and will soon be the standard IP signalling mechanism for both multimedia and voice calling service [9]. As time goes on, the older Private Branch Exchanges (PBXs) and network switches will be outdated and replaced with SIP enabled network model that is packet switched and IP based. [10]

2.1.2 H323

[4] Described H323 as an International Telecommunication Union (ITU) standard that transmits audio and video signal over a packet switched network. It was published in 1996 and it is referred to as an umbrella standard that encompasses several other protocols which includes H.225 RAS signaling, H.225.0 call signaling (Q.931), H.245 Control signaling and others.[11]. This means that it is not a protocol itself but what it does is to define how to use other protocols. [6].

Protocols relating to H323 are binary protocol based on ANSI standard 1. It uses SRTP (Secure Real-Time protocol) as a standard protocol for confidential media transport and Multimedia Internet Keying (MIKEY) for exchanging keys. [12]. It is very important to note that signalling protection is only guaranteed up to the gateway. Each of the H323 protocols has its specific role in calls process setup and all but one are made up of dynamic port. The H323 is composed of several endpoints like the gateway, gatekeeper and the back end service.

III. Common Attacks Launched On VoIP Network

The customary security vulnerable in data network can affect the voice communication and needs to be guarded against. The following present the different types of attacks that can occur when making or receiving a call;

3.1 Theft of service and abuse

This type of attack is mostly directed towards the service provider where malicious user uses the service fraudulently with an intention of not paying for it. [12]. There are various methods the hacker can use in achieving this fraudulent task. In its simplest form of toll fraud, the attacker places call using an unused IP phone by impersonating the identity of the rightful user of the telephone. In a more complex scenario, the attacker may place a rouge IP phone in the network or an unauthorized call can be made by bridging the gateway.

3.2 IP Spoofing

[13] Described spoofing as forging parts or entire packet so as to look as if it's coming from the rightful source. This occurs when an attacker disengages a phone and takes up the identity of the VoIP client [14]. This can be achieved in two different ways; the hacker can either use the IP address within the trusted range of IP addresses for a network or an authorized external IP address that is trusted and has right to some specified resources in the network. IP spoofing attack can also be used to lunch other type of attacks like the denial of service (DoS) attack that uses spoofed source address to hide the identity of the hacker. [11].

3.3 Masquerading

This is the pretence of an entity to be another entity. [15]. It takes place when the hacker within or outside a network pretends to a remote user as the rightful recipient when in fact his having a conversation with the hacker. This usually occurs in cases where the hacker assumes the place of someone that is not well known to the target. Masquerading attack normally includes one or the other forms of active attack. [9]

3.4 Call interception

This is the act of unlawfully monitoring voice packets or RTCP transmission. This type of attack can be linked to wiretapping in a packet switched network where hackers captures and analyze voice packet payload when it's being transmitted over the IP network. Hackers can make use of data sniffing and other well known hacking tools to detect, alter, store and playback the captured voice packets because voice travels in packets over the data network. [12].

3.5 Call Hijacking

This is the act of hijacking or redirecting an ongoing conversation to a different end point.[16]. The hacker could swap the original voice mail address with the hacker's IP address thereby opening a channel for the hacker.[17]. In this case, all the VoIP calls will not reach its intended destination. Similar tools used in launching call interception are used in achieving call hijack.

3.6 Denial –of Service (DoS)

[18] claimed that DoS attack is the most harmful VoIP attack due to the fact that it has a direct impact on customers and results in loss of productivity, revenue and system downtime. This attack prevents the valid users of the network from using the features and the services of the network. The major way of launching this type of attack is by flooding the network or server with spurious traffic with the intension of overloading it. This causes serious degradation of the network with unavailability of service [19].

IP phones and Gateways can also be subjected to flooding attack in an attempt to disrupt voice communication.[12] Identified the ping command which uses ICMP (Internet Message Control Protocol) as one of the major means of carrying out flooding attack. TCP SYNC could also be used to achieve a similar outcome. Due to the fact that DoS attack can be carried out from any location by anybody, it's very difficult to mitigate.

3.7 Eavesdropping

Eavesdropping in VoIP is quite different from that of the conventional eavesdropping in a data network. Eavesdropping in VoIP occurs when a voice packet is intercepted by the attacker using programs like VOMIT (Voice over Misconfigured Internet Telephony). [20].This enables the attacker to listen to voice conversation without the knowledge of the target. [21].The network requires a physical access to ensure interception of signalling and media stream conversation. Separate network protocol like UDP or TCP is used for signalling messages and ports from media itself. Media streams are transmitted over UDP using RTP (Real Time Protocol)

IV. Introduction To VoIP Security

[22] Identified the internet as the future of voice communication and some other IP applications. Any technology implemented with data packets of any type over the internet are always a subject of security concern which is majorly because of the open nature of the internet.[20] .People always want to feel secured in everything they do and voice communication is not exceptional. Security in VoIP is now a major concern with news headlines like "Venezuelan VoIP hacker imprisoned for 10 years after stealing over 10 million minutes of VoIP call and selling them again for profit". VoIP network which is essentially an IP network inherits the same security issue which is common to any IP network because of their open nature. [3].

4.1 Effect of security on QoS

Due to the real time nature of voice, the security implemented on the traditional Data network is not applicable to it because of its low tolerance to delay and packet loss.

In deploying security on the VoIP network, the quality of service (QoS) must be put into consideration.

[23] Identified QoS as essential in the operation of the VoIP network. [24] Then admitted that there will be degradation in the QoS of voice after implementing security on the VoIP network. [25] Identified blocking or denying of call setup that leads to delay and latency as one of the consequence of implementing security on VoIP.

[26] Then provided a solution to the worrying security deployment by recommending some specially made security solutions for voice traffic consisting of an inbuilt QoS mechanism. He also made other recommendations like encrypting packets at end point, using a Secured Real Transport Protocol (SRTP) for transmitting voice and video application and providing a reasonable amount bandwidth that will be sufficient for the intended applications.

4.2 IPSec and Encryption

Voice encryption in IP network has become essential due to the open nature of the internet. [27] Described the easy capturing of voice packets using packet sniffing and some other known techniques as the major reason why transmitted packets have to be secured. VoIP security has become a major concern and must

be solved in two directions, first by protecting what the caller is saying (Encryption) and also authenticating the receiver of the call.
IPSec is a suite of security protocol and encryption algorithm that is used in securing IP packets against both authorized and unauthorized person that captures packets that are not meant for them on the network. Therefore [28] stated that it is practical and logical to introduce IPSec to VoIP, encrypting the voice packet at one end and decrypting when it gets to the intended recipient at the other end.

4.3 VPN Tunnelling using IPSec

[29] Defined Virtual Private Network (VPN) as a security deployment on a shared infrastructure that has the same security policy as that of the private network. VPN is a tunnel configured between two network nodes that provide a secured path for transmitting information. This information transmitted is encrypted to provide data integrity and confidentiality. The VPN tunnel that supports multiple protocols implemented within a corporate LAN or WAN is better secured and faster than the one implemented over the internet. IPSec being the most commonly used for the VPN tunnelling will be implemented.

4.4 VPN tunnelling configuration using IPSec

In the implementation phase of this study, an asterisk box was first configured in other to have a platform where our designed security can be implemented on. A little summary of how the asterisk box was configured will be briefly discussed before elaborating on the security implemented.

V. Asterisk

Asterisk is an open source Voice over IP solution invented by Mark Spencer of Digium Inc in 1999. Because it can run conveniently on mid range PC hardware and its open nature as compared with other commercial VoIP deployment, it has become a choice of VoIP users. Asterisk runs on Linux platform and was released under GNU General Public Licence.

Asterisk runs on UNIX operating system and can be accessed through the command line interface (CLI). Various version of Asterisk has been developed after it was released in 1999 with the latest being Asterisk 1.8 released in 2010. It has more than 200 notable new features which include new security features, more than 200 enhancements, integration with IPv6 and lots more. Asterisk supports protocol like IAX, SIP, H323, SCCP and MGCP. SIP protocol was used in this study

5.1 Configuring Asterisk

In configuring Asterisk, two different approaches can be deployed; these can be either configuration method by manually editing or the Graphic User Interface (GUI) using point and click. The manual editing was used for this study.
During the configuration process, the following files where manually edited;
Sip.conf: In this file the various sip clients were defined in their context for the Asterisk PBX.
Extensions.conf: This file defines how calls are handled and routed within and outside the Asterisk box. The dial plan for various users is also defined in their context that determines how they interact in the Asterisk.
Voicemail.conf: This file defines an interaction interface with callers when the intended receiver is not available to receive the call.
To check the status of the configured users, its extension number, IP address, port number and status, the command used is ***#sip show peers***; this is illustrated in figure 1

Figure 1. VoIP network configuration using Asterisk

In designing security for the VoIP network between two sites, the following client choices were adopted.
1. **VoIP platform**: Asterisk
2. **Choice of Protocol**: Session Initiation Protocol (SIP)
3. **Security choice**: VPN tunnel using IPSec

1.2 VPN tunnelling using IPSec implementation Choice
The process involved in achieving this has been streamlined into five main steps:
1. Declaration of interesting traffic: Declaring interesting traffic helps to initiate the whole IPSec process. Traffic is termed *interesting* as soon as the configured IPSec policy begins the IKE (Internet Key Exchange) process. The declaration of interesting traffic is part of security policy formulation the VPN uses. This determines the specific traffic that needs encryption during transmission. Access list here defines cryptography policies that uses either the permit or deny statement. The permit statement specifies the traffic that needs to be encrypted while the deny statement specifies the traffic that should be transmitted unencrypted.

2. IKE phase 1: The rationale behind IKE phase 1 is the setting up and authentication of a secured channel between two IPSec peers so as to enable IKE exchanges. The following occurs during IKE phase I:

- The IPSec peers identity are protected and authenticated
- IKE exchange is protected by negotiating a matching between the IPSec peers.
- Authentication of Diffie-Hellman exchange key with the intension of matching the shared secret keys.
- Setting up of a secured tunnel that negotiates IKE phase 2 parameters.

Two different types of mode exist in IKE phase I, the main mode and aggressive mode.
In the main mode, two way exchanges occur three times between the caller and the receiver when a call is initiated. During the first exchange, a common matching hash and algorithm is agreed on by both of the peers for the purpose of matching IKE SAs. The second exchange generates a shared secret key using Diffie-Hellman exchange. The numbers sent at random to the second party helps to prove its identity. The third exchange of the main mode verifies the identity of the other side. What identifies this identity is the encrypted IP address of the IPSec's peer.

The main function of the main mode is to provide a secured pipe by matching IKE SAs (Security Association). Values specified by IKE SA during IKE exchange includes: the type of authentication method used, hash algorithm and encryption method, Diffie-Hellman group applied, the life time and the shared secret key used for the encryption algorithm.

Aggressive mode is composed of fewer packets and little exchanges are made here. During the process of the first exchange, majority of the packets are compressed into the recommended IKE SA values. The major disadvantage of using this mode is because the two sides exchange information before the initiation of a secured channel. It is much faster than the main mode.

3. IKE Phase 2: The purpose of IKE phase 2 is to setup IPSec tunnel by negotiating IPSec SAs. The following process is carried out during this phase:
- Negotiation of IPSec SA parameters that is protected by an existing IKE SA.
- Establishing IPSec security association.
- Negotiation of IPSec SA periodically to ensure security
- Additionally performs Diffie-Hellman exchange. (optional)

The IKE phase 2 operates in only one mode which is the quick mode.

4. IPSec Encrypted Tunnel: After the successful completion of IKE phase 2 and IPSec SA has been established by quick mode, packets are exchanged through the IPSec tunnel. The transmitted packets are encrypted and decrypted using 3DES specified in the SA

5. Tunnel Termination: The IPSec tunnel terminates by either timing out or deletion. An SA times out went the specified number of seconds is attained or when the stipulated number of byte has passed through the tunnel. Whenever the SA terminates the key are disposed. When another IPSec SA is needed for transmission, IKE performs a new phase two or phase one negotiation if required. New SAs can therefore be established before the expiration of the existing one so as not to interrupt transmission.
After the VPN configuration, ***#show crypto isakmp sa*** was used to verify if the tunnel has actually been created for transmission of the voice packet.

After the verification the creation of the VPN tunnel, the command ***#show crypto ipsec sa*** was used to verify the encryption and decryption of packets at the source and destination.

2. Testing the IPSec VPN Tunnel Using Wireshark

In testing the IPSec VPN tunnel, a scenario was setup by introducing a switch in-between the two routers that connects the two sites. This switch was also connected to a computer running wireshark software. Wireshark is a very powerful tool used by network administrators to monitor packets in a network. It can also be used to troubleshoot network issues. Despite all the benefits it posses to the network administrator, it can also be used by hackers to monitor packets illegally with the aim of stealing user logins and password, capturing voice packets, sniffing , eaves dropping and lots more.

In this scenario, we used wireshark in monitoring voice packet when an IPSec VPN was not configured between the sites and when the tunnel was configured for transmission of voice packets

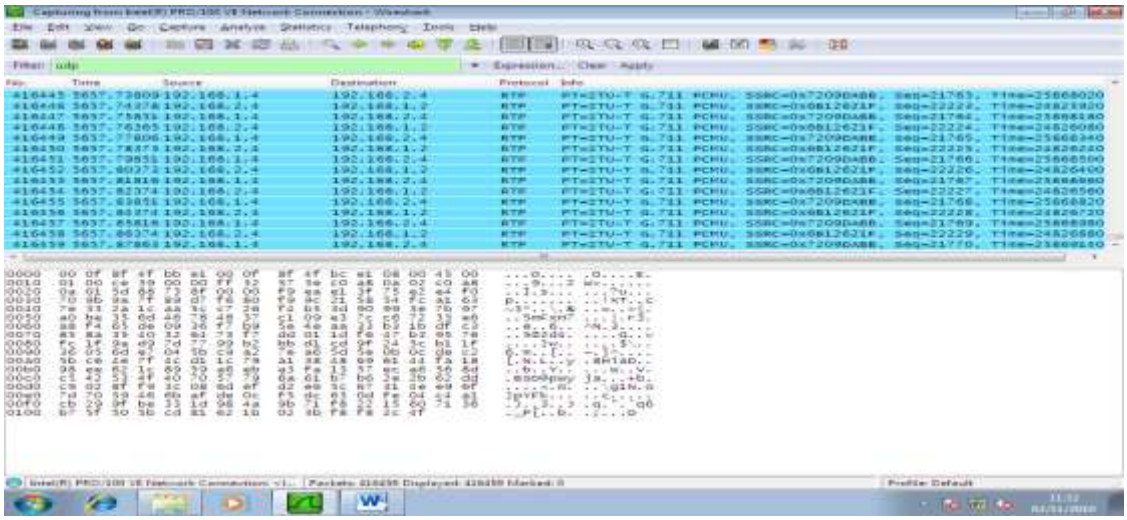

Figure 2 Screen shot illustrating the captured voice packets when VPN tunnel was turned off using a wireshark.

In figure 2 above, it can be noticed that after setting up a conversation when the VPN tunnel was turned off, a live capture was taken using wireshark software and lots of vital information was revealed concerning the call. Among these are the source and destination of where the call is coming from and going to (*192.168.2.4 to 192.168.1.4*), the type of protocol used (*RTP*), the payload type (*ITU-T*), the type of codec used (*G.711*), Synchronization Source Identifier (SSRC), Sequence number and the timestamp.

All these information's are very sensitive and aids the hacker when carrying out an attack on the VoIP network

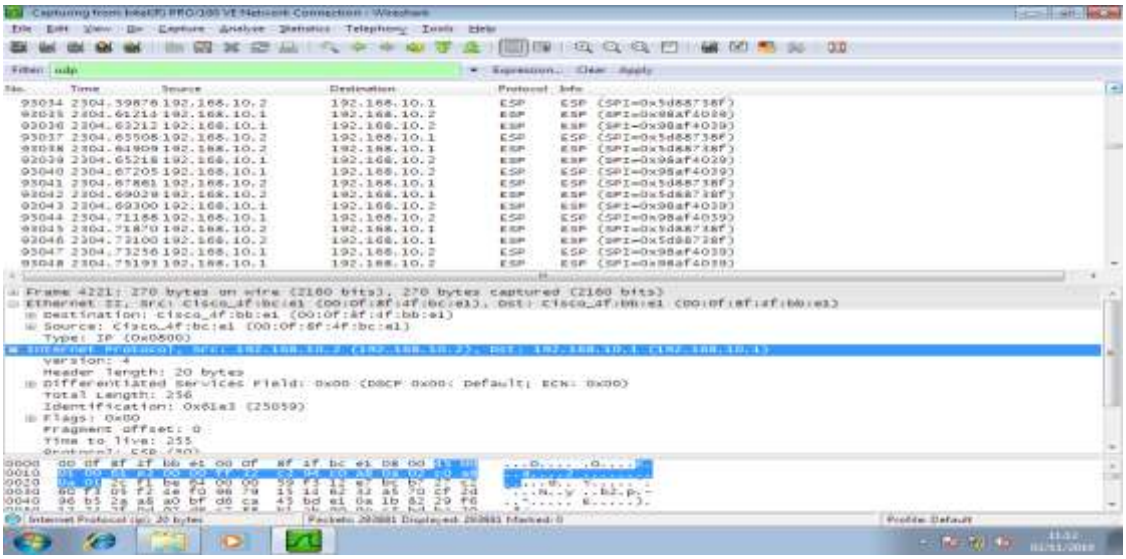

Figure 3 Result obtained when VPN tunnel was activate

In figure 3 above, it can be observed that the source and destination IP address of where the call was established and terminated has been hidden and replaced with the serial link IP address (*192.168.10.1- 192.168.10.2*), therefore it is impossible for the hacker to detect the call's source and destination address. The protocol type and other information has also been encrypted to ESP (*Encapsulating Security Payload*) leaving the hacker with no meaningful information.

VI. Conclusion

The future of VoIP technology depends on how secured it is. It will be considered to totally replace the traditional PSTN if it can guarantee confidentiality, integrity and availability on both private and public network. Some authors have tried to describe a way of securing VoIP network but most of the solutions are not practicable, therefore this paper presents a practical solution that encrypts voice packets in a VoIP network. This was achieved by first deploying a Voice over IP system using an open source Asterisk on a Linux platform before going on to configure a VPN tunnel between two users in different site. A thorough testing of the VPN was carried out using wireshark software to analyze the effect of not having VPN connection and having VPN connection.

It was then observed that without the implementation of the VPN tunnel across the two sites, the voice packet being transmitted will be exposed to easy attack by hacker. Therefore implementing security over VoIP network is essential.

References

[1] Hallock, J. (2004) *A brief history of VoIP, Evolution and Trends in Digital Media Technologies*, University of Washington

[2] La Corte, A., & Sicari, S. (2006), 'Assessed quality of service and voice and data integration: a case study', *Computer Communications*, 29(11). pp. 1992-2003.

[3] Ranganathan, M. & Kilimartin, L. (2003) 'Performance analysis of secure session initiation protocol based VoIP networks', *Computer Communications* 26(6), pp. 552-565.

[4] Amarandei-Stavila, M. (2005) *Voice over IP Security A layered approach*, xmco partners.Amoroso, E. (1994) *A book introducing critical issues in computer security technology*, *Fundamentals of Computer Security Technology*, Bell Laboratories.

[5] Karapantazis, S. & Pavlidou, F. (2009) 'VoIP: A comprehensive survey on promising technology', *Computer Networks*, 53(12), pp.2050-2090.

[6] Ansari,S. , Khan ,K. , Rehana,J. , Lisa,J. , & Kaisar, S. (2009) 'Different Approaches of Interworking between SIP and H323' *International journal of Computer Science and Network Security*, 9(3),pp.232-239.

[7] Geneiatakis, D., Lambrinoudakis, C. & Kambourakis, G. (2007) 'An ontology-based policy for deploying secure SIP-based VoIP services', *Computer & Security*, 2006(27), pp.285-297.

[8] Wisely, D. (2001)'SIP and conventional internet application' *BT Technology journal*, 19(2), pp.107-118.

[9] Stallings W., (2003) 'The Session Initiation Protocol', *The internet protocol journal*, 6(1), pp.5-38.

[10] Borthick, S. (2003) *SIP for the Enterprise: Work in Progress*, *Business Communications Review*.

[11] Porter,T., Baskin, B., Chaffin, L., Cross, M., Kanclirz, J., Rosela, A., Shim, C.,& Zmolek, K. (2006). *Practical VoIP Security*. Syngress Publishing Inc. Rockland MA.

[12] Fernandez, E., Palaez, J., & Larrondo-Petrie, M. (2007) 'Security Patterns for Voice over IP Networks', *Journals of Software*, 2(2), pp. 19-29.

[13] White, G.,Archer, K., Core, J., Cothren, C., Davis, R., DiCenso, D., Good, T., & Williams, D.(2001) Voice and Data Security,1st edition, Indianan: Sams Publishing.

[14] Brownridge,G ., LeVay, L., Rybczynski, T. (2005) 'Protecting VoIP and multimedia communications from growing security threats', *Nortel Technical Journal*

[15] Rossebo,J. & Sijben, P. (2006) 'Security issues in VoIP' ,*Telektronikk*,102(1), pp.23-26

[16] Ramirez.,D (2007) 'Security Within VoIP Networks', *Information Systems Control Journal*, Vol 6, pp. 41-42.

[17] Greenfield, D. (2004) 'Securing the IP Telephony Perimeter' Network magazine. Available at:http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=18900070

[18] Bhan, S., Clark, J., Cuneo, J., & Mejia-Ramirez, J. (2006) *Information Security Issues in Voice over Internet Protocol*. Available at http://users.ecegatech.edu

[19] Onofrei, A., Rebahi, Y. & Magedanz,T. (2010) 'Preventing Distributed Denial-of-Service Attacks on the IMS Emergency Service Support through Adaptive Firewall Pinholing' *International Journal of Next Generation Network* ,2(1), pp. 1-17

[20] Ghafarian, A., Draughorne,R., Hargraves, S., Grainger, S., High, S., & Jackson. (2007) 'Securing Voice over Internet Protocol' *journal of information Assurance and Security*, 2(2007), pp 200-204.

[21] Chochol ,P. (2009) 'Qualitative Factors that impact real implementing VoIP in private network' , *Acta Electrotechnica et informatica* ,9(4), pp. 61-65.

[22] Casteel, J. (2005) *Sound Choice for VoIP Security*. Available at:http://www.ebcvg.com/pdf/dl/sound_choices_voip_security.pdf

[23] Ansari ,S. & Khan, A. (2007) 'Voice over Internet Protocol Security problems in Wireless Environment' *Journal of Engineering and Sciences*, 1(2),pp. 82-85.

[24] Chen ,X. , Wang,C. , Xuant, D. , Li,Z. ,Min,Y. , & Zhao,W. (2003), 'Survey of QoS Management on VoP', *in proceeding of the 2003 international conference on Computer Networks and Mobile Computing*, Institute of Chinese Academy of Sciences.

[25] Elbayoumy,A. & Shepherd,S. (2007) 'A Comprehensive Secure VOIP Solution' *International Journal of Network Security* , 5(6), pp.233-240.

[26] Kuhn, D.,Thomas, J. ,Walsh, Steffen, F.(2005) National Institute of Standards and Technology; NIST Recommendations of NIST concerning VoIP security; *Security Considerations for Voice over IP Systems*.

[27] Salama, G., Sheuab, M., Hafez, A. & Zaki, M. (2009) 'Performance Analysis of Transmitting Voice over Communication Links Implementing IPSec' 13th International Conference on Aerospace Science & Aviation Technology ASAT-13.

[28] Tahir,A., & Shahzad, A .(2010) 'Security Issues for Voice over IP Systems', *International journal of computer and network security* ,2 (5), pp 41-51.

[29] Asraf, M., Davis, J., & Grout,V. (2009) 'An Investigation into the Effect of Security on Performance in a VoIP Network'. Proceedings of the Fifth Collaborative Research Symposium on Security, E-Learning, Internet and Networking SEIN 2009, 26-27 November 2009, pp. 15-28