11-1-2009

An Investigation into the Effect of Security on Performance in a VoIP Network

Muhammad T. Asraf

John N. Davies
Glyndwr University, j.n.davies@glyndwr.ac.uk

Vic Grout
Glyndwr University, v.grout@glyndwr.ac.uk

An Investigation into the Effect of Security on Performance in a VoIP Network

Abstract
Voice over Internet Protocol (VoIP) is a communications technology that transmits voice over packet switched networks such as the Internet. VoIP has been widely adopted by home and business customers. When adding security to a VoIP system, the quality of service and performance of the system are at risk. This study has two main objectives, firstly it illustrates suitable methods to secure the signalling and voice traffic within a VoIP system, secondly it evaluates the performance of a VoIP system after implementing different security methods. This study is carried out on a pilot system using an asterisk based SIP (Session initiation Protocol) server (Asterisk, 2009).

Since VoIP is intended for use over the Internet, VPNs (Virtual Private Networks) have been used in a tunnel configuration to provide the service. Additionally the performance of networks level IPSec (Internet Protocol Security) and application level ZRTP (Zimmerman Real Time Transport Protocol) security have been compared with no security. Registration, call setup and voice transmission packets have been captured and analysed. The results have then been extrapolated to the Internet.

Keywords
voice over IP, quality of voice, soft-phones, asterisk open source PBX software, MOS, SIP, RTP

Disciplines
Computer Engineering | Digital Communications and Networking

Comments
This paper was presented at the Fifth Collaborative Research Symposium on Security, E-Learning, Internet and Networking (SEIN 2009), 26-27 November 2009, which was held in Darmstadt, Germany. It was published by the University of Plymouth and the symposium proceedings are available at http://www.cisnr.org

An Investigation into the Effect of Security on Performance in a VoIP Network

Muhammad Tayyab Ashraf , John N. Davies and Vic Grout

Centre for Applied Internet Research (CAIR)
Glyndŵr University, University of Wales, Wrexham, UK
s07003692@stu.newi.ac.uk,{j.n.davies|v.grout}@glyndŵr.ac.uk

Abstract

Voice over Internet Protocol (VoIP) is a communications technology that transmits voice over packet switched networks such as the Internet. VoIP has been widely adopted by home and business customers. When adding security to a VoIP system, the quality of service and performance of the system are at risk. This study has two main objectives, firstly it illustrates suitable methods to secure the signalling and voice traffic within a VoIP system, secondly it evaluates the performance of a VoIP system after implementing different security methods. This study is carried out on a pilot system using an asterisk based SIP (Session initiation Protocol) server (Asterisk, 2009).

Since VoIP is intended for use over the Internet, VPNs (Virtual Private Networks) have been used in a tunnel configuration to provide the service. Additionally the performance of networks level IPSec (Internet Protocol Security) and application level ZRTP (Zimmerman Real Time Transport Protocol) security have been compared with no security. Registration, call setup and voice transmission packets have been captured and analysed. The results have then been extrapolated to the Internet.

Keywords

Voice over IP, Quality of voice, Soft-phones, Asterisk open source PBX software, MOS, SIP, RTP

1. Introduction

VoIP (Voice over Internet Protocol) is a technology used to transmit voice conversations using the IP (Internet Protocol) over a network using packets of data. The data network can be an Intranet or more likely the Internet and so has changed the strategy adopted by telecommunication managers. It is therefore one of the highest growth areas. Due to the convergence of communications technologies into IP, companies are investing more and more time and money into researching this technology area so that legacy telephone systems can be replaced. The aim of the conversion is to reduce the costs to home and business users by standardization of the network infrastructure. Most houses and business these days have continual use of the Internet and have sufficient bandwidth via broadband services to make it feasible to use for voice calls. The popularity of VoIP is increasing rapidly due to cheap calls worldwide. Skype the free VoIP provider has registered 400 million user accounts at the end of 2008. It is now expected that there will be 56 million active VoIP users around the globe by the end of 2009 (Heywood, 2009).

'Pots' (the Plain old telephone system) uses the PSTN (Public Switch Telephone Network) to support communications and utilizes circuit switching. A dedicated point to point circuit is established between the caller and the receiver in order to make a call and this circuit remains dedicated until the end of the conversation. During a call, no other network traffic can use those allocated switch channels.

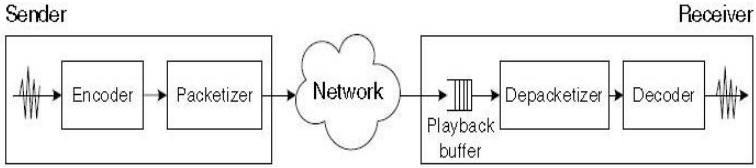

Figure 1 Components of a VoIP system

On the other hand data networks utilize packet switching and so a dedicated circuit does not exist, a virtual circuit is created, making the network much more efficient. Voice information is sampled and converted to digital form before being assembled into packets which are transmitted over the IP network. Each data packet contains the source and destination IP address and is routed to the destination using the level 3 routing mechanism prescribed in the network. At the destination these packets are then disassembled and played to the user as seen in Figure 1.

Since VoIP is based on computer systems it is vulnerable to security attacks in the same way as any other computer system. There are many ways in which the security of a VoIP system can be exploited. (Benini and Sicari, 2008) As far as the call process is concerned there are three main areas that can be exploited, call setup, voice conversation and the termination of the call. Security mechanisms can be applied to the call setup process as well as the voice transmission to reinforce identification and authentication mechanisms. To protect the information transmitted some techniques employ encryption algorithms or apply cryptographic functions to the packet payload. Unfortunately this can have an adverse effect on the network since it introduces delay, jitter and lost packets into the overall network. The stronger the algorithm the greater the level of security and the greater the corresponding effect on the network. Clearly this can affect the end to end QOS (quality of service) to the user and so it is important for network designers to have some guidelines.

This paper investigates security problems that exist and possible techniques that can be used to protect the system from them. In particular it concentrates on two techniques, the use of a VPN (Virtual Private Network) using the level 3 protocol IPSec, (Phifer, 2001) and the use of application level protection using ZRTP (Zimmerman Real Time Transport Protocol) (Zimmermann et al., 2009) to provide the security. Measurements are then made on a pilot network and comparisons are made with measurements taken on the same network without a security technique applied. These results are then scaled up to identify the typical numbers that are safe to use in the Internet. Figure 2 shows applications of VPNs.

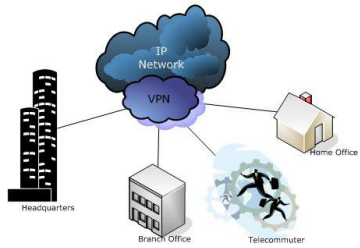

Figure 2 Typical usage of VPNs

2. Background to VoIP Security

Before looking at the issues associated with VoIP security it is worthwhile having a brief look at the non VoIP Systems i.e. the existing POTS since this is an indication of the basic problems that need to be addressed.

2.1. Threats and Attacks in a Non VoIP System (PSTN)

The public switched telephone network is also susceptible to many threats and attacks the major being toll fraud, wire tapping and attacks on modems.

2.1.1. Toll Fraud

In toll fraud the attackers can place a standard call and use Dual Tone Multi-Frequency (DTMF) tones to access and manipulate PBXs, Interactive Voice Response (IVRs), Automatic Call Distribution (ACDs), and other systems in order to eliminate the cost of long-distance calls. By war dialling, attackers find lines and codes that provide a second dial tone, which they use to commit toll fraud. Since VoIP uses a different signalling system then this technique is rendered redundant.

2.1.2. Wire Tapping

Wire tapping is the monitoring or interception of a telephone conversation by physically accessing the telephone wire. Depending on the laws of the country getting caught doing this can be a very serious crime. Generally this has to be carried out with inside knowledge but is very simple to carry out since once the circuit has been identified then an earpiece can give access to the whole conversation. Since the voice conversation in VoIP is transmitted in packets then this process is made much more difficult.

2.1.3. Attacks on Modems

Dialup modems are still used in many networks usually as backup systems to be used in fault conditions in networks. Remote users attempt to gain access to computer system by dialing the modem. If precautions are not taken to secure the modem then the system becomes vulnerable to attack. VoIP makes this technique redundant

2.2. Threats and Attacks in a VoIP System

As with many of the security issues associated with computer systems the reason for carrying this out is either to gain advantage - e.g. money or information, at other times it is carried out as a challenge. Fortunately due to the techniques used by VoIP there is a certain amount of built in security.

2.2.1. Spoofing

This type of attack can be best described as the "*man in the middle attack"* (Porter & Gough, 2007). Unauthorized persons or a program spoofs or pretends to be someone they are not with the aim of toll fraud, gaining access to messages and obtaining useful information such as bank details, PIN numbers etc. Call forwarding is a feature of forwarding incoming calls from one phone and can also be targeted by attackers. VoIP service elements - e.g. SIP proxy - and can be accessed and the configuration to route the calls on different numbers changed in an attempt to commit toll fraud.

2.2.2. Interception or Eavesdropping

Even though VoIP Networks transmit voice packets without encryption it is not simple to listen to telephone conversations. For this type of attack the unauthorized person must be between the two end users otherwise it is not possible for a hacker to capture the traffic. An unauthorized person with a packet sniffer could capture the VoIP packets but having captured the data then the process of interpreting the data is not simple. Initially it is necessary to select the correct packets and match them up with packets travelling in the opposite direction, which could be taking a different route. Due to the compression techniques normally used the data would have to be played through the appropriate codec for this to be intelligible. The purpose is to obtain user identity, SIP phone numbers and PIN (Gold, 2009).

2.2.3. Denial of Service

DoS use two types of attacks to collapse the entire VoIP system. The first is by sending the distorted or damaged packets to crash the VoIP system and the other is by sending a flood of well formed packets to exhaust the resources. DoS attacks can occur at two layers of the OSI model either on the application layer or transport layer. At the application layer, DoS attacks by sending a flood of call invitations or by sending registration requests at the signalling channel and if this attack is on the media cannel then DoS attack floods large volumes of call data which consumes large amounts of bandwidth. In both the cases the genuine users are unable to make calls (Chen, 2006).

2.2.4. Spam over VoIP

VoIP is vulnerable to spam also known as SPIT, (spam over Internet telephony) (Ahson & Ilyas, 2009). This type of spam attack can also disable the whole VoIP system. Not only does the VoIP user receive a lot of unwanted calls every day but also VoIP spam can attack the gateway and degrade the quality of voice.

2.3. Security Methods

There are techniques that can be applied to address the various attacks described in section 2.2. For Pots the methods adopted require the addition of equipment e.g. firewalls and Secure Terminal Equipment which all involve extra cost. However the solutions for VoIP involve either the reconfiguration of equipment used to protect the data network or the use of different protocols or applications which generally do not cost money but cost in terms of performance (Dantu et al., 2009).

3. VoIP Security Process

As with the standard circuit switching process of the PSTN, VoIP also has a three phase approach. Call setup, transmission of the voice information and breakdown of the call.

3.1. VoIP Registration and Call Setup

Security issues associated with call setup are twofold - to gain free calls and to block the system to prevent other users from using the network. The same concerns apply to call breakdown (hang up).

Before a VoIP call can be established it is necessary to register with the PBX i.e. this registration process ensures that the user is connected to the network available to make or accept calls. Generally this process is protected by passwords and can be limited to specific addresses (MAC and or IP addresses). The users normally register with the PBX as part of the start up process of the application on the client machine.

The dominant protocol for VoIP networks to set up calls is the Session Initiation Protocol (SIP) developed by the IETF (Internet Engineering Task Force) RFC 3261. It is a text-based protocol and is similar to HTTP which is used in Web services. SIP supports both UDP and TCP transport layer protocols but UDP is dominant due to the reduced overhead (Rescorla, 2004).

A number of protocols can be used to provide integrity, confidentiality and authentication of SIP signalling messages. These protocols include the use of IPSec, TLS, S/MIME, DTLS and HTTP digest authentication. The selection and adopting of the security protocol is normally dependant on the ease of use and scalability of the implementation. HTTP digest authentication is the simplest method where a message digest key or hash function is used as a digest authentication to protect the shared secret key during the SIP session negotiation (Johnston, 2004).

The IPSec protocol is widely used particularly in a SIP environment since it gives protection to applications that use UDP or TCP. It can be used in transport mode or in tunnel mode to secure the payload. The way that IPSec is used in this investigation is to create secure tunnels between the end devices in order to provide integrity, confidentiality and authentication for signalling and media messages. (Johnston & Piscitello, 2006)

3.2. Transfer of Voice Traffic

In the UK it is illegal to listen to private conversations; specifically it is unlawful to listen to conversations of people who use either PSTN phones or VoIP phones to make calls. Though it is difficult for a person to capture and interpret the voice packets from the Internet it cannot be completely ignored. The standard media protocol which is used to exchange voice streams is Real time Transport Protocol (RTP) (Schulzrinne, et al., 2003).

3.2.1. VPN and IPSec

A Virtual Private Network (VPN) is defined as "network connectivity deployed on a shared infrastructure with the same policies and security as a private network". It is possible to create a tunnel over a standard IP network (Internet) that supports multiple protocols and therefore extend the security of the private network to remote offices or telecommuters. The VPN is configured between two networks or end systems providing confidentiality via encryption, data integrity to ensure the data has not been altered and authentication to certify the source of the information (Figure 3).

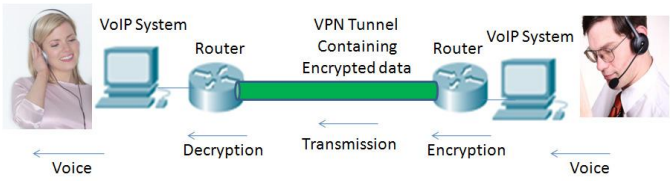

Figure 3 The use of VPN with IPSec

It is possible to implement VPN protection at different layers. When one layer is encrypted, then by definition all layers above it are protected so network layer protection has become the most popular level to apply cryptographic protection to network traffic. The IP Security Protocol (IPSec) is the most commonly used protocol at level 3 that provides this functionality so this paper concentrates on this (Cisco, 2007).

3.2.2. Application Level Protection

Since it is possible to provide protection at the application layer and there is no real standard to do a comparison on the performance it was decided to choose a typical application, Zfone. This uses ZRTP (Zimmermin RTP) messages which are embedded into RTP packets as added extensions ignored by an end-point unless it supports ZRTP. It utilises the Diffie-Hellman key exchange mechanism to derive a common key between two communicating parties. The key exchange occurs after the signalling has taken place (SIP and SDP). This solution is provided by the specific VoIP application that sits on top of the TCP/IP stack. Whenever a new VoIP call is negotiated, the application negotiates a new encryption key between the parties and then encrypts the VoIP packets on the fly.

3.2.3. Methods to secure Network for VoIP

In order to make the secure VoIP system, the surrounding network environment should also be protected by using the techniques normally employed in data networks. Segmentation of entire VoIP networks plays a vital role in controlling the traffic between the different components of a VoIP system. The same techniques used in the data network can be employed. This segmentation of the network can be done physically or logically depending upon the requirement. The traffic can be filtered with the use of different network elements such as routers, switches and firewalls.

Private IP addressing schemes also provide security to the VoIP network from external attacks. A Network Address Translator (NAT) server which maps the internal private IP addresses to the public IP addresses in order to route the traffic to the outside world can be used. VoIP firewalls are also used to protect the system from the attackers by filtering the inbound and outbound traffic. Policies are made for the whole VoIP traffic and implemented in the firewalls.

There are two types of intrusion detection systems which are used to prevent intrusion, signature based and anomaly based ID systems. Signature based IDS checks the individual packets and matches them with the known signatures to identify the malicious attack. Anomaly based IDS analyze the combined streams of network traffic and performs pattern matching based on predefined traffic heuristics to identify the attacks. The IDS is typically configured to look for a specific function in a protocol e.g. UDP, TCP, and HTTP (Palmieri, 2009).

4. Performance of VoIP System

The Quality of Service provided to the end user is of upmost importance and one of the main issues for the implementation of VoIP system, since if the conversation is unintelligible then there is no point in providing the service. The main factors that affect the quality of service are Latency, Jitter and Packet loss

4.1. Latency

This is the delay for packet delivery from source to destination and is a general problem in all telecommunication networks. In VoIP latency depends upon the delays created by encoding, packet production, physical network and routing delays, play back and decoding. Encoding delay depends upon the codec used to encode the voice signal. Packet creation delay is the time it takes to create the RTP packets from the encoded voice stream. Network delay is the sum of propagation, transmission and queuing delay. Playback delay is a result of the playback buffer on the receiver side and the decoding delay is the time the system takes to reconstruct the original voice signal. The recommended value for total delay by ITU (International Telecommunication Union) for good quality is 150ms from source to destination. The delay is acceptable from 150-300ms. If delay is greater than 300ms then it must be reduced.

4.2. Jitter

Jitter is the variation in delay for packet delivery and occurs due to improper queuing and network congestion. The information is broken down into packets and then these packets travel from source to destination, maybe by different paths. The arrival of these packets varies depending on network utilisation. The acceptable value of jitter for good voice quality is 20-50ms. If the value of jitter is greater than 50ms then the quality of voice will be poor.

4.3. Packet Loss

Packet loss occurs due to many factors but the usual cause is network congestion. The transport level preferred by most VoIP networks is UDP (user datagram protocol) which is a connectionless protocol and so lost packets are a feature of the protocol since packets will not be retransmitted. Similarly if a packet is not received on time then it will be discarded by the VoIP application.

4.4. Effect of Security on VoIP Performance

Methods for securing the VoIP system discussed previously are all likely to affect the performance by increasing the latency, jitter and/or packet loss. Encryption algorithms apply cryptographic functions to the packets and introduce delay for the encryption and decryption of voice packets, the stronger the algorithm the greater delay. Security mechanisms also increase call setup delay due to the identification and authentication mechanisms. Security mechanisms can also increase delay and jitter during the call when the VoIP packets pass through them. IPSec security is implemented in the routers to provide the secure tunnel for traffic between the end users. Similarly other security protocols such as ZRTP, SRTP and TLS also induce delay in packets. It is necessary to investigate the overall affect of these on the system.

5. Investigation & Analysis

The investigation was carried out by implementing a pilot network using the same equipment and conditions so that a comparison could be made with some level of confidence in the result. Three tests were chosen including VoIP without security, with IPSec security and with ZRTP protocol. These tests were carried out to analyze the effect of security on the quality of voice.

The network was designed using an Asterisk SIP server to handle the SIP calls. The X-Lite (X-lite, 2009) softphone application was configured on desktop computers with speakers and headphones for initiating and receiving the calls. The Wireshark application was installed on a separate computer to capture the voice and signalling packets passing through the network. Cisco routers and hubs are used in this network. The routers are connected to each other via fast Ethernet cable.

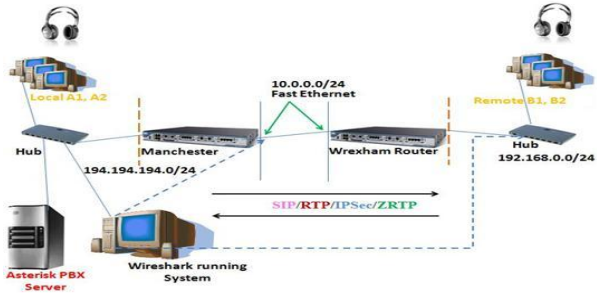

Figure 5 Network Design for VoIP Implementation

5.1. Scenarios

In the first scenario the quality of voice was checked by measuring the delay and jitter without implementing the security. Device A is local to the Asterisk PBX server and device B is remote - i.e. separated by routers. All the SIP and RTP traffic will pass through the routers insecurely. Wireshark was placed local to the Asterisk server to capture all the VoIP signalling and voice traffic. This enabled the delay and jitter to be analysed offline. Then in scenario two VPN with IPSec security tunnels were implemented on the routers. All the signalling and voice traffic initiated by the end devices and Asterisk servers were encrypted and decrypted by the routers (Figure 6). In scenario three, security is provided at the application level using the ZRTP application layer protocol was used provide end to end encryption to secure the VoIP traffic. The Zphone utility was used for the implementation of ZRTP on the local and remote devices for end to end encryption.

5.2. Analysis

As discussed in Section 3 results were taken for the registration process, call setup and the transmission on the voice traffic to ensure that there is no adverse affect on one phase more than the other. Packets were captured using Wireshark and then exported into a spreadsheet to enable offline analysis to be carried out. For the voice traffic captures were taken over a period of several minutes and so a histogram was made of the results.

5.2.1. Registration Process

The first step in the process is for the X-lite clients to register the user with the Asterisk server. The graph shown in Figure 6 is the representation of the SIP traffic which is initiated by the devices for the registration with Asterisk SIP server.

It can be seen from Figure 6 that for the remote client to register in an unsecured VPN setup there is a sharp peak around 0.005msecs whereas with IPSec security employed then a delay is introduced and with ZRTP due to the processing required by the client machine the overall time is larger than the unsecured. Even so the whole process only occurs on the start up of the application and lasts for a maximum of 0.038msec so it is not going to have any significant effect on the network.

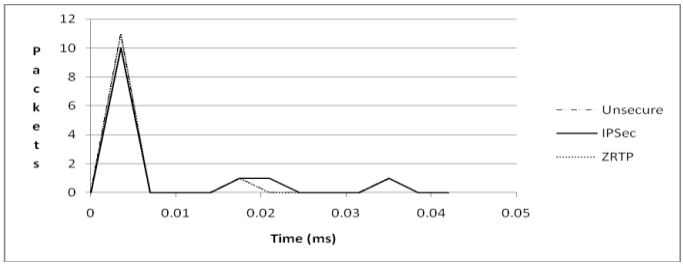

Figure 6 Comparison of Registration Process for Remote Client

5.2.2. Call Setup

Figure 7 shows the comparison graph for call setup process from remote the VoIP device to the local VoIP device using SIP. The graph is same for both unsecured and ZRTP. The unsecured packets have been sent in a time of 0.05ms and with a delay of 4ms. The same number of average packets has been sent with IPSec security but this shows a time of 1ms but with an increased spread and one packet experienced a delay of 7ms indicating that IPSec increases the length of time taken for the setup.

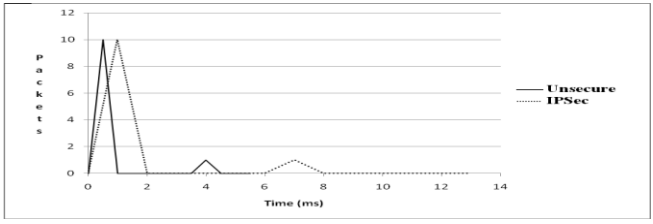

Figure 7: Comparison of Call setup times

Again this is not really significant since the call setup only takes place once at the beginning of the call and the worse case time is 7 msecs. The process is initiated by the user and so in human terms it would not be noticed.

5.2.3. Voice Traffic between End Devices A & B

Figure 8 shows the comparison graph for RTP traffic between local and remote VoIP clients. The percentage difference, based on average times for packets between unsecure and IPSec, is 13% and, between Unsecure and ZRTP, is 11%.

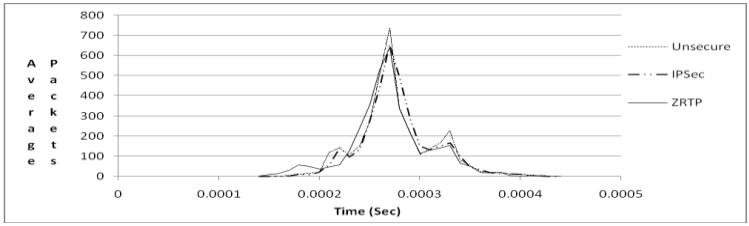

Figure 8: Comparison of Voice Traffic

5.2.4. Delay & Jitter in RTP Streams

Calculations can be made from the graph shown in Figure 8 which can be supported by the information provided by Wireshark in summary Table 1.

	RTP Traffic	Average Delay	Average Jitter	Standard Deviation	Min Jitter	Max Jitter	Total Jitter
Unsecure	A - B B - A	19.99 19.99	2.17 2.26	1.93 1.98	0.02 0.04	7.88 8.16	4.43 (ms)
IPSec	A - B B - A	20.05 20.00	2.34 2.63	2.08 2.11	0.01 0.16	8.07 14.19	4.97 (ms)
ZRTP	A - B B - A	19.99 20.02	2.28 2.38	1.97 1.95	0.07 0.07	8.13 8.15	4.64 (ms)

Table 1 Average Delay & Jitter between Local & Remote

5.2.5. Extrapolation from Results

Based on the results obtained in Section 6.4 calculations can be carried out to investigate the effect that this might have on the use of this type of security through the Internet. These can be seen in Table 2. From previous measurements with the use of the Traceroute utility it has been found that a typical number of routers that are passed through when accessing a web-server on the Internet is 5 and so this has been used as a limit.

No. of Routers	2	2	5	5	5
No. of Users	2	5	10	20	30
Delay (ms)	20	40	100	100	100
Jitter (Unsecure)	2.17	10.85	21.7	43.4	65
Jitter (IPSec)	2.34	11.7	23.4	46.8	70
Jitter (ZRTP)	2.28	11.4	22.8	45	68.4
Performance	Excellent	V. Good	Good	Fair	Poor

Table 2 Effect of Users & Routers on the Performance

Values for delay and jitter recommended by the ITU for good quality have been used to provide a range of performance grades from excellent to poor in Table 2.

Delay	< 150ms	>150ms < 300ms	> 300ms
Jitter	< 20ms	> 20ms < 50ms	> 50ms
Packet Loss	< 1%	> 1% < 5 %	> 5 %
Performance	Excellent	Good	Poor

Table 3 ITU Recommended Values for VoIP Quality

6. Conclusion

When compared to the plain old telephone system VoIP is quite a secure service which justifies the integration with the data network. However there are issues that need to be addressed to improve the overall security of the network and the VoIP service. Since the use of Virtual Private Networks can run on public and private networks it is a good strategy to adopt to improve the security of the service when passed over the Internet is a very good strategy to adopt despite the usability and performance issues.

Usability is not always straightforward when adopting a VPN strategy since there are many options available and they require varying levels of skills for the user. However by adopting a protocol like IPSec at the network layer has the advantage that it will protect any application.

Having investigated the performance issues with VPN, the signalling i.e. registration, call setup and call breakdown are insignificant in overall times of the call. But when VPN used in even in an unsecured manner this will have an effect on the network performance on the voice traffic transmitted and hence the QoS experienced by the end to end users. Based on the calculations for a network with 10 users using VoIP run on low end routers implemented on a 100Mbps LAN to get a good QoS the network should be limited to a maximum transit through 5 routers based on the ITU recommended value for delay and jitter.

When securing the network with IPSec over the VPN then the percentage difference for average jitter between unsecured and IPSec is 4% due to the overheads encountered in the routers. If security is carried out at the application layer using a specialized application which utilises a protocol like ZRTP the percentage difference when compared to an unsecured VPN is 2.2%.

6.1. Future Enhancement

In this study DES encryption standard and pre-shared keys have been used during the implementation of IPSec. Many other encryption standards i.e. 3DES, AES, RSA, hash algorithms are available with IPSec which could have been used to change the level of security used. Two operation modes of IPSec can be used i.e. transport mode and tunnel mode. Only the tunnel mode was used in this study. The transport mode

of IPSec could be used in future to secure & analyse the traffic. It is hoped that Asterisk will be available with ZRTP support in future which could be used to analyse the data when the signalling is secured and voice traffic of VoIP.

It is anticipated that support for security at other levels e.g. TLS (Transport Layer Security) which provides strong authentication, integrity and message privacy will arrive in new versions of PBX and IP phones. The use of SRTP (Secure RTP) that provides security to RTP streams only and doesn't secure the SIP signalling traffic could also be investigated. SRTP could be used with IPSec to provide the end to end results.

7. References

Ahson, Syed A. & Mohammad Ilyas, (2009) VoIP Handbook, CRC Press, 2009 pp.372

Asterisk (2009) http://www.asterisk.org/about accessed at 04/04/2009.

Benini M, Sicari S, (2008) Assessing the risk of intercepting VoIP calls Computer Networks 52 (2008) 2432–2446

Chen, E. Y. (2006), "Detecting DoS attacks on SIP systems," 1st IEEE Workshop on VoIP Management and Security, 2006, pp. 53–58.

Cisco Networking Academy (2007), CCNP 2: Remote Access Module, Chapter 13 Virtual private Networks

Dantu R, Fahmy S, Schulzrinne H, Cangussu J, (2009), Issues and challenges in securing VoIP, Computers & Security Vol 28 (2009) 1–11

Gold S. (2009), European Union to investigate Internet telephony eavesdropping, Infosecurity Europe 2009

Heywood, T. (2009) A Brief History of VoIP, ezinearticles.com/?A-Brief-History-of-VOIP&id=2141357

Johnston, A. B. (2004), SIP: Understanding the Session Initiation Protocol, 2nd Ed., Artech House Telecommunications Library.

Johnston, A. B. & David M. Piscitello(2006), Understand VOIP security, , Artech House, 2006 pp.103- pp.107

Palmieri F, Fiore U, (2009), Providing true end-to-end security in converged voice over IP infrastructures, Computers & Security 28 (2009) 433 – 449

Phifer, L. (2001), VPNs: Virtually Anything? A Core Competence Industry Report, http://www.corecom.com/html/vpn.html.

Porter, T. & Gough, M., (2007) VoIP Security, by Syngress Publishing, Inc., 2007 pp. 58, 81

Rescorla, E, and Modadugu N (2004), Datagram Transport Layer Security, June 2004, IETF Internet-Draft, www.ietf.org/Internet-drafts/draft-rescorla-dtls-05.txt.

Schulzrinne H, Casner S, Frederick R, and Jacobson V (2003), RTP: a transport protocol for realtime applications, IETF, RFC 3550.

X-lite(2009) http://www.x-lite.com/

Zimmermann, P. Johnston A. and Callas J, (2009), Internet Draft to the IETF for the ZRTP http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-15