International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 2, pp: (476-486), Month: April - June 2015, Available at: www.researchpublish.com

VOIP Pros and Cons

[1]Roopa Dinakar Patil, [2]Tejashree Ravikant Sawakare

[1,2]A.S.M's Institute of Management & Computer Studies Plot C-4, Wagle Industrial Estate,
Near Mulund Check Naka, Opp. to Aplab, Thane (W) – 400604 India.

Abstract: **Voice over the Internet protocol (VOIP) is being rapidly deployed, and the convergence of the voice and data worlds is introducing exciting opportunities. Lower cost and greater flexibility are the key factors luring enterprises to transition to VoIP. Some security problems may surface with the widespread deployment of VoIP. In this article, we discuss these security problems and propose a high-level security architecture that captures required features at each boundary-network-element in the VoIP infrastructure. We describe mechanisms to efficiently integrate information between distributed security components in the architecture.**

Keywords: **VoIP security, Threats, Feedback, VOIP attacks, Security solutions**

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VoIP services require a computer or a dedicated VoIP phone, while others allow you to use your landline phone to place VoIP calls through a special adapter. Voice over IP refers to the diffusion of voice traffic over internet-based networks. Internet Protocol (IP) was originally designed for data networking and following its success, the protocol has been adapted to voice networking. The history of VoIP began with conversations by a few computer users over the Internet. Initially, VoIP required a headset to be plugged into the computer, and the participants could only speak with others who had a similar set up. They had to phone each other ahead or sent a text message, in order to alert the user at the other end of the incoming call and the exact time.

In the mid-90s, IP networks were growing, the technology had progressed and the use of personal computers had grown extensively. The belief that VoIP could start to make some impact on the market resulted in high expectations and the distribution of the first software packages. In its early stages, the technology was not sufficiently mature. There was a big gap between the marketing hype and the technological reality, resulting in an overall agreement that technical shortages stopped any major transition to VoIP. However, VoIP has continued to make technical and commercial progress and most of the technical problems have been solved, while others arose. Now its presence is no longer restricted to a limited market niche The fundamentals of this technology have been around since the mid-1990s. Since then, VoIP (also known as IP telephony) has been one of the most important trends of the future for the telecommunications industry and for years has been the subject of numerous reports in industry and business media. While the heralded communications revolution initially took almost a decade to arrive, it has undoubtedly been picking up speed since around 2005.

2. VOIP PROTOCOLS

In this section firstly we will discuss VoIP protocols and data processing in VoIP and quality of service in VoIP systems. There are currently three protocols widely used in VoIP implementations- the H.323 family of protocols, the Session Initiation Protocol and the media Gateway Controller Protocol (MGCP). VoIP vendors are current selling solutions that can work with either of these families of protocols.

A. H.323 Family of Protocols:

H.323 is a set of recommendations from the International Telecommunication Union (ITU) and consists of family of protocols that are used for call set-up, call termination, registration, authentication and other functions.These protocols are transported over TCP or UDP protocols. The following figure.1 shows the various H.323 protocols with their transport

mechanisms. H.323 family of protocol includes H.225 is used for registration, admission, and call signaling. H.245 is used to establish and control the media sessions and T.120 is used for conferencing applications in which a shared whiteboard application is used. The G.7xx series of specifications defines audio codec used by H.323,

while the H.26x series of specifications defines the video codec. H.323 uses RTP for media transport and RTCP for control of the RTP sessions.

The following figure.2 & figure.3 shows the H.323 architecture and call set-up process.

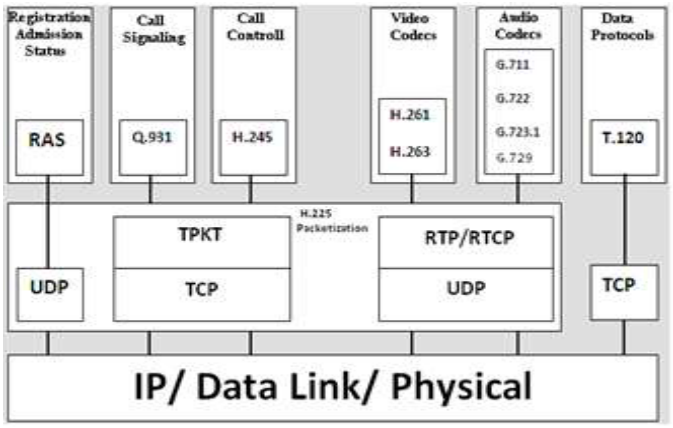

Figure 1: H.323 Protocol Family

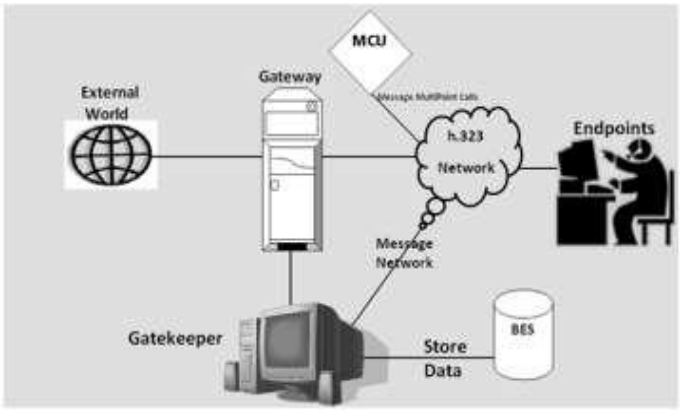

Figure 2: H.323 Architecture

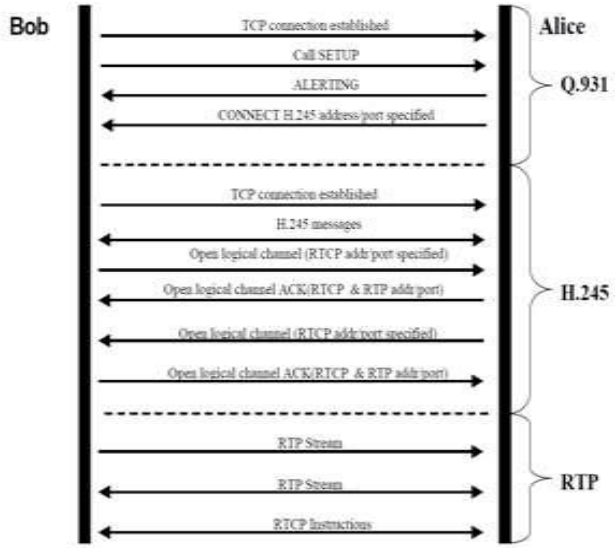

Figure 3: Call Setup Process in H.323

B. Session Initiation Protocol (SIP):

The Session Initiation Protocol (SIP) was defined by the Internet Engineering Task Force (IETF) for creating, modifying and terminating sessions between two or more participants. These sessions are not limited to VoIP calls. The SIP protocol is a text-based protocol similar to HTTP, and offers an alternative to the complex H.323 protocols.

Due to its simpler nature, the protocol is becoming more popular than the H.323 family of protocols.

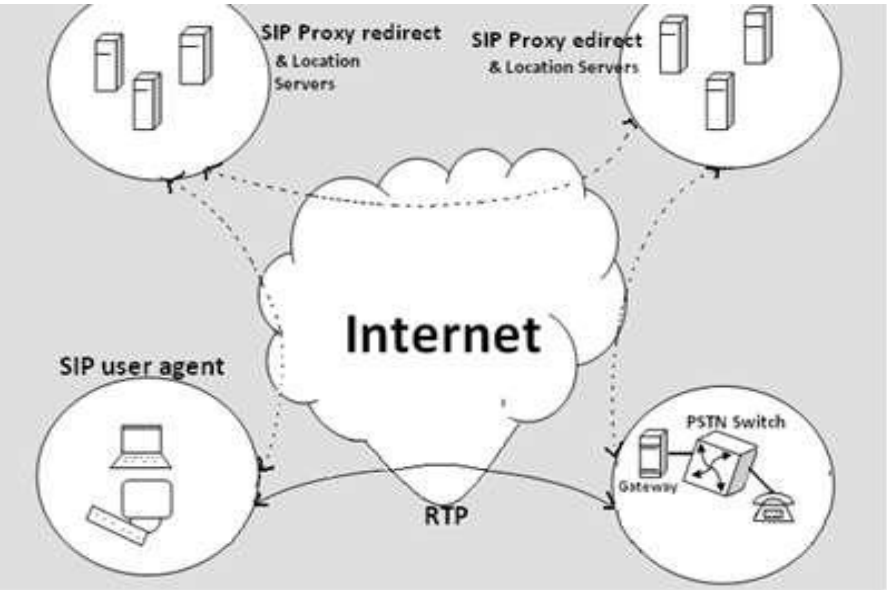

Figure.4 shows the SIP architecture and call set-up and tear down process.

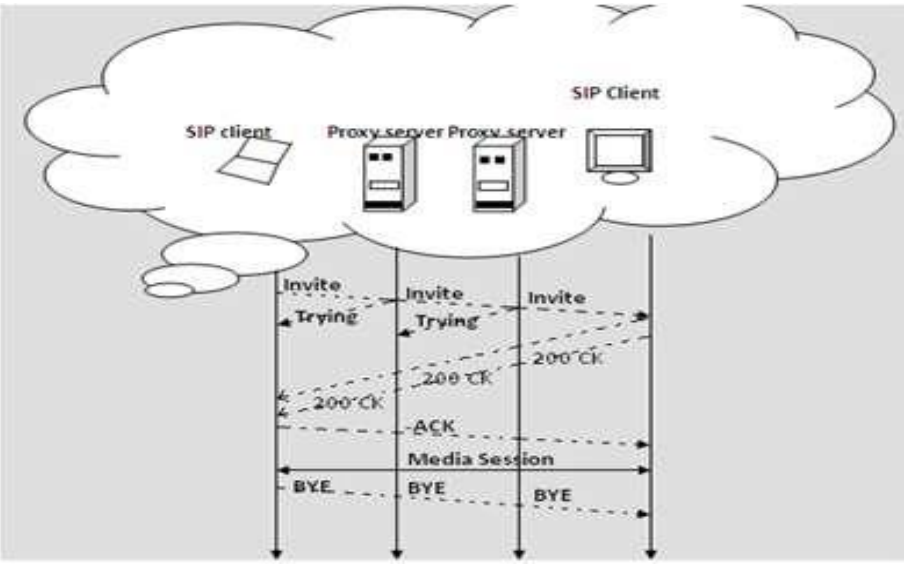

Figure.5 SIP Network Architecture Figure 5: Call setup and tear down in SIP

C. Media Gateway Control Protocols (MGCP):

MGCP is used to communicate between the separate components of a decomposed VoIP gateway.

It is a complementary protocol to SIP and H.323.Within MGCP the MGC server or "call agent" is mandatory and manages calls and conferences, and supports the services provided (see Figure 6).

The MG endpoint is unaware of the calls and conferences and does not maintain call states. MGs are expected to execute commands sent by the MGC call agents. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under their control. MGCP does not define a mechanism for synchronizing call agents. MGCP is a master/slave protocol with a tight coupling between the MG (endpoint) and MGC (server).

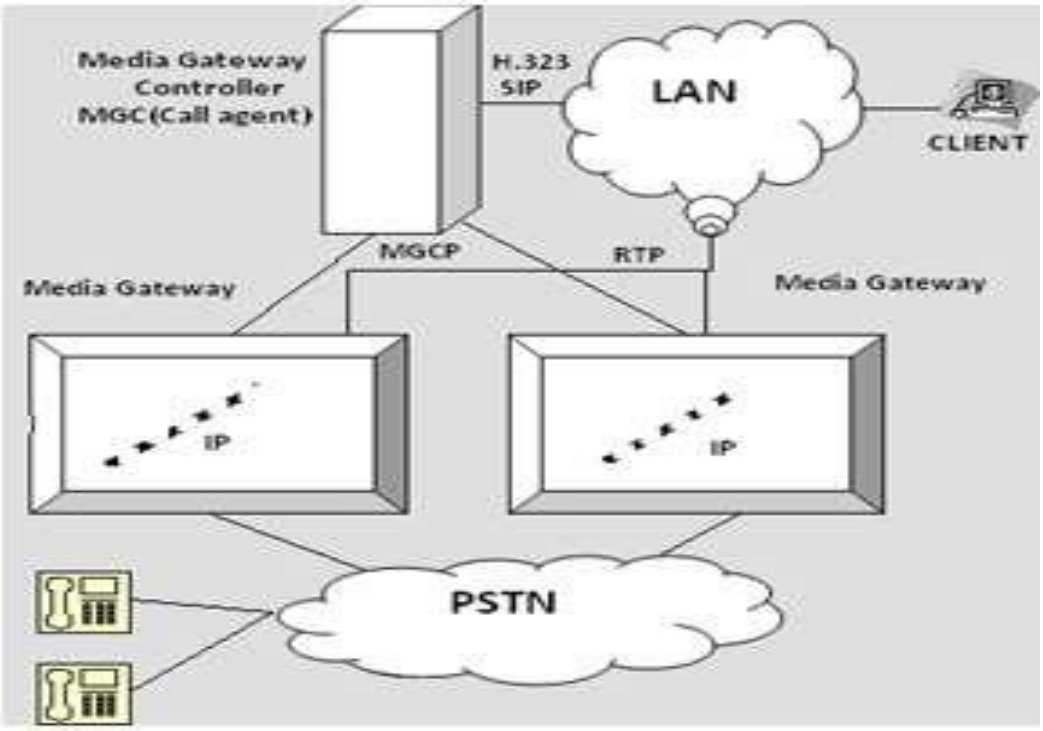

Figure 6: MGCP Architecture

3. IMPLEMENTATION OF VOIP PROTOCOLS

A. Data Processing in VoIP Systems:

VoIP consists of three essential components: CODEC (Coder/Decoder), packetizer and play out buffer. At the sender side, an analog voice signals are converted into digital signals, compressed and then encoded into a predetermined format using voice codec. There are various voice codecs developed and standardized by International Telecommunication Union-Telecommunication (ITU-T) such as G.711, G.729, and G.723 etc. Next packetization process is performed which fragment encoded voice into equal size of packets. Furthermore, in each packet, some protocol headers from different layers are attached to the encoded voice. Protocols headers added to voice packets are of Real-time Transport protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP) as well as Data Link Layer header. In addition, RTP and Real-Time Control Protocol (RTCP) were designed at the application layer to support real-time applications. Although TCP transport protocol is commonly used in the internet, UDP protocol is preferred in VoIP and other delay sensitive real-time applications. TCP protocol is suitable for less delay-sensitive data packets and not for delay-sensitive packet due to the acknowledgement (ACK) scheme that TCP applies. This scheme introduces delay as receiver has to notify the sender for each received packet by sending an ACK. On the other hand, UDP does not apply this scheme and thus, it is more suitable for VoIP applications.

The packets are then sent out over IP network to its destination where the reverse process of decoding and de-packetizing of the received packets is carried out. During the transmission process, time variations of packet delivery (jitter) may occur.

Hence, a play out buffer is used at the receiver end to smoothen the play out by mitigating the incurred jitter. Packets are queued at the play out buffer for a play out time before being played. However, packets arriving later than the play out time are discarded. The fig.7 shows the end –to- end transmission of voice in VoIP system.

Besides, there are signaling protocols of VoIP namely Session Initiation Protocol (SIP) and H.323. These signaling protocols are required at the very beginning to establish VoIP calls and at the end to close the media streams between the clients.

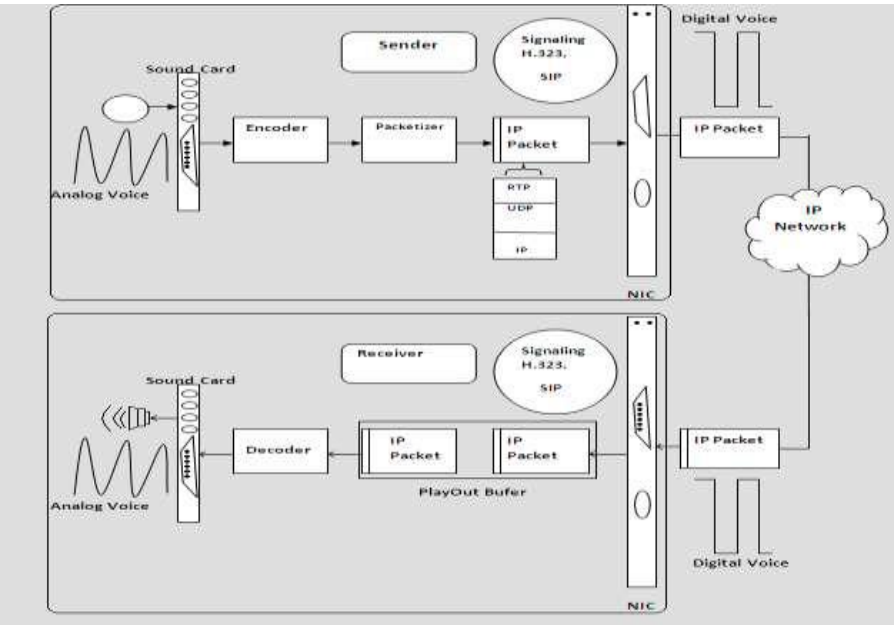

Figure.7 End-to End Voice Transmission

B. Quality of Service (QoS) in VoIP Systems:

Quality of service (QoS) can be defined as the network ability to provide good services that satisfy its customers. In other words, QoS measures the degree of user satisfactions; the higher the QoS, the higher degree of user satisfaction. QoS are briefly described in following sections.

1) Delay: Delay can be defined as the total time it takes since a person, communicating another person, speaks words and hearing them at the other end. Delay can be categorized into: delay at the source, delay at the receiver, and network delay

2) Jitter: IP network does not guarantee of packets delivery time which introduces variation in transmission delay. This variation is known as jitter and it has more negative effects on voice quality.

***3) Packet Loss*:** Packets transmitted over IP network may be lost in the network or arrived corrupted or late. Packets would be discarded, when they arrive late at the jitter buffer of the receiver or when there is overflow in jitter buffer or router buffer. Therefore packet loss is the total loss occurs due to network congestion and late arrival .In case of packet loss, the sender is informed to retransmit the lost packets and this would cause more delay and thus affecting

4) Transmission QoS.: Echo In VoIP, Echo is experienced when caller at the sender side hears a reflection of his voice after he talked on the phone or the microphone whereas the cal lee does not notice the echo. Echo is the term of the reflections of the sent voice signals by the far end. Echo could be electrical echo which exists in PSTN networks or acoustic echo which is an issue in VoIP networks

5) Throughput: This parameter concerns about the maximum number of bits received out of the total number of bits sent during an interval of time.

4. CONFIGURATIONS OF VOIP

A. Dedicated routers:

These devices allow any user to use its own traditional phone to place VoIP calls. They are connected to cable/DSL modems (or any high-speed internet source) and allow any user to attach an ordinary telephone. Once these routers are configured with an appropriate VoIP provider and service plan, There is no need of special software or interaction with computer. In fact, there is only need to pick up your phone and dial a number at the dial tone. You can also bring your own adapter with you when you travel and make calls wherever broadband internet access is available.

B. Adapters (USB):

USB devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters that are slightly larger than the typical thumb drive. They feature a standard modular phone jack to which you

can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service.Software-controlled VoIP applications: "soft phones" There are many software applications ("soft phones") that allow you to place VoIP phone calls directly from an ordinary computer with a headset, microphone, and sound card. Internet telephony service providers usually give away their soft phones but require that you use their service.

Together, these applications and services enable users to talk to other people using the same service at no cost, and to the rest of the world for a fee. Software-based VoIP applications are quite attractive to consumers because they often already have most of the components necessary to get started at little to no cost.

C. Dedicated VoIP phones:

A VoIP phone looks like an ordinary corded or cordless telephone, but it connects directly to a computer network rather than a traditional phone line. A dedicated VoIP phone may consist of a phone and base station that connects to the internet or it may also operate on a local wireless network. Like the VoIP adapters mentioned above, dedicated VoIP phones also require a provider as well as a required service plan.

5. ADVANTAGES AND DISADVANTAGES OF VOIP

A. Advantages:

There are so many advantages to using VOIP that I almost don't even know where to begin. By far the biggest advantage to using VOIP is the cost savings. There are a lot of different VOIP systems available and the amount of money that you will save really just depends on which system you invest in. Some VOIP systems will only allow you to make calls to others who are running VOIP, while other VOIP systems will allow you to call anyone who has a phone. Typically, PC to PC VOIP calls are free, aside from the initial cost of the software and a possible monthly service fee. PC to phone calls typically cost more than PC to PC calls, but are still usually less than half of the cost of phone to phone calls. Most VOIP providers who support PC to phone calls charge a small monthly fee for unlimited calls within the United States. A very small premium typically applies to international calls .As you can see, the cost of VOIP service really just depends on your service provider. The same can be said of the calling features. Most service providers include features such as call forwarding, call waiting, and three way calling with their VOIP service. These are far from being the only available features though .Some VOIP services are computer based, meaning that you speak through a microphone that is connected to a computer. Computer based VOIP environments tend to be highly collaborative. It is not at all uncommon for a computer based VOIP system to be able to transmit video in addition to voice so that you can see and hear the person that you are talking to. Computer based VOIP systems often also allow you to share data and / or applications with the person that you are talking to, thus allowing collaboration on a project. Of course there is no reason why these collaborative sessions have to be limited to two people. Most computer based VOIP systems support conference calling. Not all VOIP systems require the use of a computer though. Some simply use a digital VOIP phone or a VOIP adapter that can be used with a regular telephone. There are several advantages to using a VOIP phone rather than a computer based VOIP application. Probably the biggest advantage is simplicity. Placing a VOIP call over a VOIP phone is usually no more complicated than placing a normal phone call. Another advantage is portability. A VOIP phone has an address built into it that is unique to your phone. This means that in most cases, you can take your VOIP phone with you and use it anywhere that a broadband Internet connection is available. Obviously, there are exceptions, but generally speaking you could take your VOIP phone with you on a trip to California even if your service was based in New York. You don't necessarily need a VOIP phone to get portability. Some providers of computer based VOIP services offer a Web interface. This interface allows customers to log in and place calls from anywhere in the world, so long as a broadband Internet connection is available. This should be a serious consideration if you have employees that travel a lot and make a lot of calls from the road. The service isn't as convenient as a cell phone, but it is usually a whole lot less expensive and it works in foreign countries where a cell phone may not.

B. Disadvantages:

As great as VOIP technology is, there are some major disadvantages that you have to consider prior to investing in VOIP. The biggest issue plaguing VOIP is sound quality. Don't get me wrong though, with sufficient bandwidth and good equipment, it is possible to get fairly good sound quality from a VOIP system. In real world conditions though, there are no guarantees that the sound quality will be acceptable. There are a couple of different reasons for the sound quality issue. The first reason has to do with the way that VOIP works. As I mentioned earlier, VOIP stands for Voice Over IP. To see how this can be a problem, think about how an IP network works in regards to transmitting data. When a file needs to be

sent over an IP network from point A to point B, the file is broken up into a series of packets. The packets are transmitted in a sequential order, but because of the distributed nature of the Internet, the packets may arrive at their destination in order, or they may be out of order. Normally, this isn't a problem because the recipient is able to use the packet's sequence number to figure out what order the packets go in, and reassemble the data. VOIP converts voice into digital data, which is then placed into packets and transmitted over the internet. As with any other type of data, these packets may or may not be in the correct order when the recipient receives them. The recipient's VOIP system can reassemble the packets regardless of what order they arrive in. However, the real time nature of voice conversations means that if the packets arrive out of order, then it could result in a second or two of silence while the data is reassembled. As you can see, latency issues can cause some major issues for VOIP systems. Data must be able to travel to the recipient quickly enough that it can be reassembled before anyone notices a significant delay. Since a lack of available bandwidth can cause such problems for VOIP systems, VOIP manufacturers have taken steps to reduce bandwidth requirements. Specifically, bandwidth requirements have been reduced through the use of various compression algorithms. However, these compression algorithms have caused some problems of their own. One problem is compatibility. When it comes to PC to PC VOIP calls, there is no one universal standard. Some VOIP systems are proprietary in nature, and will only allow calls to others who are using the same software. Another problem with compression is that compression (and decompression) consumes extra processing power. Furthermore, compressing the data tends to further degrade sound quality. Some compression algorithms have actually been known to cause problems with echoes. These echoes can be filtered out, but doing so requires even more processing power. Compressing and filtering data is more of an issue for computer based VOIP than for VOIP phones. VOIP phones handle the necessary compression and / or filtering at the hardware level. The advantage of this is that you never have to think about how much processing power your VOIP phone has, but it does mean that a VOIP phone can be more expensive than a regular phone. Aside from the various sound quality issues, there are also a few practicality issues that you need to consider. For example, if you are considering a computer based VOIP system, then you must remember that you will not be able to place or receive calls unless the computer is turned on, and the VOIP software is running. Another practicality issue is that unlike a traditional phone, a VOIP system (computer or VOIP phone based) is useless during a power outage. A traditional phone can function even during a power outage because the phone company transmits electricity over the phone line. This electricity is used to power the phone (cordless phones being the exception). That way, even if the power goes out, the phone will usually still works because the phone's power is coming from a different source. VOIP works completely differently though. A VOIP phone (or a computer based VOIP system) requires external power to function. Furthermore, a VOIP system also requires the Internet to be available. Therefore, if you lose power, or if you lose Internet connectivity, VOIP will not work. One last issue that I want to mention is that the 911 service does not work properly over a VOIP phone system. Normally, when you dial 911, the phone company looks at either your phone number (if you are using a land line) or the cell tower that you are communicating through, and uses that information to put you in contact with the nearest 911 dispatcher. With VOIP systems however, the caller's location cannot be determined through traditional means. As such, dialing 911 from a VOIP system won't likely put you in contact with a local 911 dispatcher. I have recently read about an experimental program which may eventually allow VOIP calls to be routed to the correct 911 dispatcher. The concept works by looking at the caller's IP address. The reason that this is possible is because IP addresses are distributed based on geographic area.

6. VOIP ATTACKS

VoIP attacks can be divided into two categories:

A. SIP attacks and RTP attacks:

Since SIP takes significant roles of session initiation, connection and termination, we need to consider SIP attacks first.

B. Malformed Message Attack:

This is one of the most representative case using the vulnerabilities of text-based protocol. Attackers are able to cause Malfunctions of proxy server or UA by manipulating SIP headers. For instance, overflow-space, overflow-null, specific header deletion and using non-ASCII code are involved in malformed message attacks.

C. SIP Flooding Attack:

IP phones generate requests or responses to send to a specific UA, called by victim. As a result, a single UA is overwhelmed by receiving excessive SIP messages within a short duration of time, so that the UA cannot provide normal services. INVITE flooding is one of the most typical attacks. Basically, flooding attack is also the issue of IP layer. In case of INVITE flooding, however, it could be more annoying attack for the VoIP user because the one should see many call requests and hear ringing.

D. Spoofing Attack:

Two kinds of spoofing attacks are possible, IP spoofing attack and URI spoofing attack. IP spoofing attack is to forge IP source addresses in order to pretend a trusted user and IP spoofing is the intrinsic security problem in TCP/IP protocol suites and it is not in the scope of our study on VoIP security. URI spoofing attack is a particular case in malformed message attacks. The attacker who hijacked SIP messages between two UAs forges their URI field, so the attacker can hide himself from trace backs. If spoofed BYE requests (BYE DoS attack) are sent to a victim, the call will be terminated by the attacker.

7. REQUIREMENTS, AVAILABILITY AND SERVICE LIMITATIONS

When considering VoIP service, you should not assume that its features, functionality and options will equal those of traditional landlines; you should be familiar with the requirements, availability and possible service limitations of VoIP service before switching to VoIP as either a primary means of communication or an enhancement to your current services.

A. Requirements:

VoIP requires a connection to the Internet through an ISP, a VoIP service to extend the reach to traditional landlines, and VoIP software to actually place calls. Plain Old Telephone Service (POTS) requires none of these prerequisites. It is important to note that Digital Subscriber Line (DSL) internet service uses traditional phone lines for your internet connection. In this case, you already have telephone service to begin with. You may wish to weigh the expected benefits of VoIP against these costs given your current operating environment.

B. Availability due to power outages:

During a typical power outage, VoIP becomes unavailable because VoIP devices (computers, routers, adapters) usually rely on a power source to function. Traditional phone lines are usually still available during such an outage, which is a major advantage in an emergency.

C. Availability due to bandwidth:

VoIP communication nearly always requires a high-speed (broadband) internet connection for reliable functionality. Even given typical broadband connection speeds, though, service interruptions or degradation of quality is possible due to high internet traffic. For example, if you are trying to place a VoIP call while other people are using a lot of bandwidth on the same internet connection, the sound quality of your VoIP call or general VoIP availability may be affected.

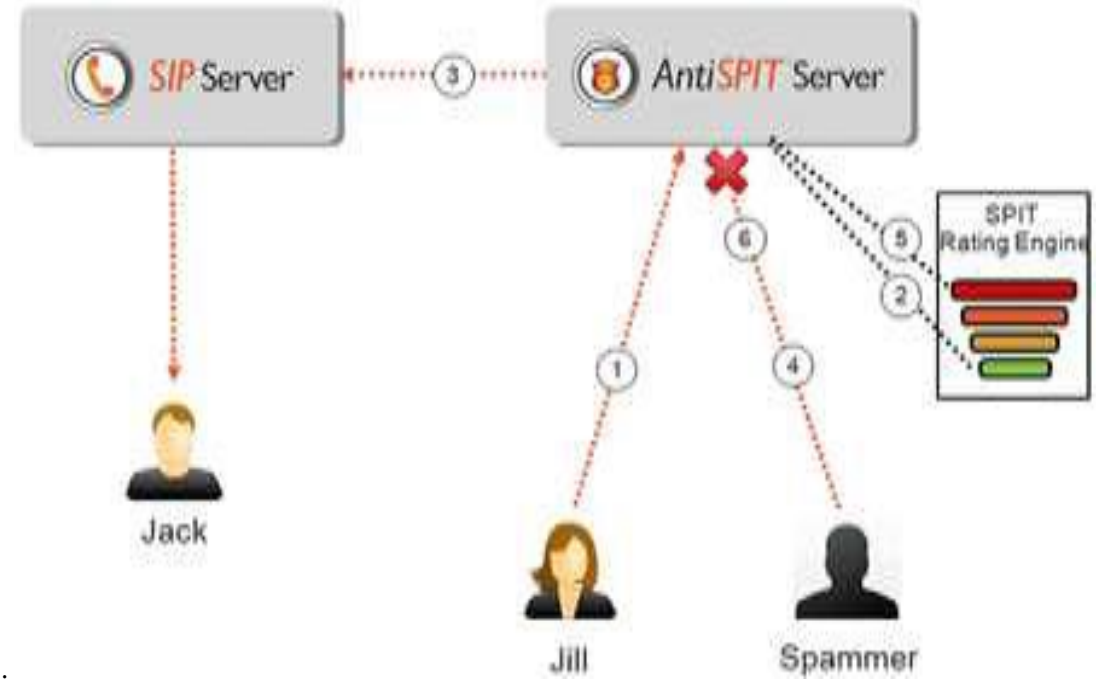

Figure.8 SIP & SPIT server [16]

8. SOLUTIONS

The "Voice VLAN" is a special access port feature of Ethernet Switches which allows IP Phones to auto-configure and easily associate to a logically separate VLAN. This feature provided various benefits, but one particular benefit is when the Voice VLAN is enabled on a switch port that is also enabled to allow simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP Phone and the connection for both PC and Phone to be trunked through the same physical Ethernet cable.

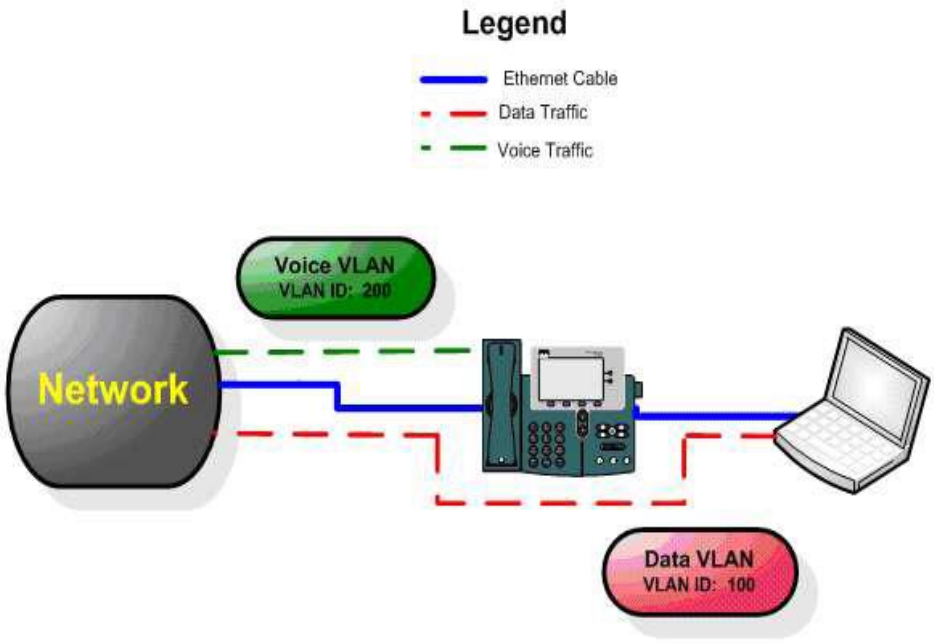

Figure 9: A typical VoIP scenario in which data and voice traffic is transmitted through the same cable

Enabling Voice VLANs raises the complexity to properly secure these physical Ethernet ports. Enabling without the proper Security controls in place can increase the risk to an organization. Many of the principles and practices for safe VoIP usage are the same as those you may already be practicing with other internet applications. Here are some of the key practices of good personal computing:

- Use and maintain anti-virus and anti-spyware programs.
- Be cautious about opening files attached to email messages or instant messages.
- Verify the authenticity and security of downloaded files and new software.
- Configure your web browser(s) securely.
- Use a firewall.
- Identify, back-up, and secure your personal or financial data.
- Create and use strong passwords.
- Patch and update your application software.
- Do not disclose personal information to people you don't know.

9. EMERGING TECHNOLOGIES IN VOIP

A. Skype:

Skype is one of the most popular VoIP applications that emphasise mostly in a voice communication in addition to a standard instant messaging such as text messages and file transfers. Skype was developed by Niklas Zennström and Janus Friis was the originators of KaZaa (one of the most popular peer-to-peer services). Skype protects the transferred data by encrypting the media channel (Porter and Gough, 2007; Wang, 2005). One of the main reasons

for the popularity of Skype VoIP services is its unique set of features to protect privacy of VoIP calls such as strong encryption, proprietary protocols, unknown codecs, dynamic path selection, and the constant packet rate (Zhu and Fu, 2010). However, some of enterprise security groups consider it as threat because it has to skip firewall in order to make call traffic. It supports call quality when establishing a connection with other Skype user. In addition, Skype got the ability to connect to any phone in PSTN (Porter and Gough, 2007; Hoßfeld and Binzenhöfer, 2008). The Skype user can communicate with anyone anywhere in the world, with either another Skype client or anyone with a phone.

B. Google talk architecture:

Google has announced that a major goal of the Google Talk service is interoperability. Google Talk uses Jabber and extensible messaging and presence protocol (XMPP) to provide real-time extensible messaging and presence events, including offline messaging (though only through non-Google clients like Adium). Google Talk now supports federation with other Jabber servers, allowing any one to send and receive IMs to other Jabber users with non-Google Talk accounts (Hester, 2009). On December 15th 2005, Google released libjingle, a C++ library to implement Jingle, "a set of extensions to the IETF's XMPP for use in VoIP, video and other peer-to peer multimedia sessions." Google Talk does not encrypt the Jabber stream, instead using an undocumented non standard way of authenticating to the service, retrieving a token from a secure web server. Other clients than Google's own are required to secure their streams with transport layer security (TLS) before sending the password, causing them to stay encrypted throughout the whole session. Google claims that all messages (text and voice) will be encrypted in future releases (Hester, 2009).

10. CONCLUSION AND FUTURE WORK

This article discusses the VoIP application security. The previous studies have shown that using VoIP increases the vulnerability of the network, as a result so many efforts has been done to overcome this problem, and to make it as less as possible. However, the low cost of the VoIP encouraged enterprises to produce many different applications that facilitate this technology, in distinct characteristics. As a result, security issues should be one of the most important things that should be taken seriously during selecting the appropriate VoIP application to be used. In this article, we studied the architecture of the VoIP and its protocols, and the security issues regarding to each level, to come with a good understanding of the security condition of the VoIP applications in the market. Finally, two different models of the VoIP application, Skype and Google Talk have been compared together, to find out which application is more reliable in terms of security. The result of comparison shows that Google Talk is more enterprise-oriented than Skype and it is open to improve its security. Skype, on the other hand, provides interesting features that Google Talk does not have at present, for instance the ability to establish a conference call with up to five people at a time and the ability to make the phone calls to mobiles and landlines worldwide at low rates. However, this software requires more bandwidth than Google Talk and it is not favorable to be used as a means of communication in business communication services. In summary, we can see that Skype is more secure in VoIP application but it does not offer interoperability. On the other hand, Google Talk has interoperability but with less level of security. It is one of the areas of the future study which fills the gap between the interoperability and security and designs the new VoIP application which offers interoperability without side tracking the security. In addition to that, security enhancement is an important factor to be considered such as a built-in antivirus protection, VoIP-aware firewalls and VoIP anomaly detection systems. In a future work, the authors might also want to consider about improving the state of the message encryption to prevent the call hijacking and eavesdropping attacks.

ACKNOWLEDGEMENT

The authors would like to thank the ASM IMCOST College of Thane for their support.

REFERENCES

[1] Sicker and T. Lookabaugh , "VoIP Security: Not an Afterthought," ACM Queue Magazine, vol. 2, pp. 56–64, September 2004.

[2] S. Vuong and Y. Bai , "A Survey of VoIP Intrusions and Intrusion Detection Systems," in Proceedings of the 6th International Conferenceon Advanced Communication Technology (ICACT), pp. 317–322,February 2004.

[3] Geneiatakis , G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas , and S. Gritzalis, "SIP Message Tampering: THE SQL code INJECTION attack," in Proceedings of 13th IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM),September 2005.

[4] G. S. Tucker, "Voice Over Internet Protocol (VoIP) and Security," white paper, SANS Institute, 2005.

[5] J. Posegga and J. Seedorf, "Voice Over IP: Unsafe at any Bandwidth?," in Proceedings of the Eurescom Summit: Ubiquitous Services and Applications Exploiting the Potential, Apri 2005.

[6] Edelson, "Voice over IP: Security Pitfalls," Network Security, vol. 2005, pp. 4–7, February 2005.

[7] Ahmed AS, Shaon RH (2009). Evaluation of popular VoIP services. 2nd International Conference on Adaptive Science and Technology

[8] Berson T (2005). Skype security evaluation. Anagram Laboratories, p.031.

[9] Camargo T (2010). Yet about Google Call. XMPP Jingle -The Next Generation VoIP. Retrieved March 12, 2011, from http://xmppjingle.blogspot.com/2010_08_01_archive.html.

[10] Cisco Systems (2002). Understanding Voice over IP Protocols. Retrieved February 5, 2011, Available at http://www.cisco.com/application/pdf/en/us/guest/tech/tk587/c1506/cc migration_09186a008012dd36.pdf.

[11] Cisco Systems (2006). Voice over ip - per call bandwidth consumption.Available at http://www.cisco.com/ application/pdf/paws/7934/bwidth_consume.pdf

[12] Dantu R, Fahmy S, Schulzrinne H , Cangussu J (2009). Issues and challenges in securing VoIP. Comput. Secur., 28(8): 743-753. Garfinkel SL (2005).

[13] VoIP and Skype security, Skype Security Overview. Retrieved April 17, 2011, from http://www.pdfking.net/VoIP-and-Skype-Security--PDF.html# Hens F, Caballero J (2008). Triple Play: Building the converged network for IP, VoIP and IPTV. John Wiley & Sons. Hester J (2009).

[14] Google Talk. Big Blue Ball.com: Instant messaging & social networking. Retrieved March 11, 2011, from http://www.bigblueball.com/im/googletalk/