Developing Best Practices for Securing VoIP Communication for a non-profit Organization

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
Networked Systems Security
December 2018
James Akinbami

Supervisors:
Seppo Virtanen
Petri Sainio

UNIVERSITY OF TURKU

Department of Future Technologies

James Akamai: Developing best practices for securing VoIP communication for a non-profit organization

Master of Science in Technology Thesis, 50 pp

Networked Systems Security

December 2018

Voice over Internet Protocol (VoIP) is the most widely used service around the world. The proficiency of it utilizing the web has increased awesome ubiquity in the current years. With this notoriety, there is expanding worry about the wellbeing of the system. The robbery or loss of the information being exchanged is great concern. For example, a basic problem for researchers who are developing safeguards for VoIP systems is the level of threats and other issues experienced by the non-profit organizations while implementing VoIP communication. This problem originated when non-profits received pressure from their donors not to implement VoIP communication because it will record important and valuable information of their bank account, including their bank balance, and consequently, exposing them to the public.

Other dangers include safeguarding secrecy, respectability, and accessibility of the system, known as CIA. dangers. To battle these dangers, some security conventions and calculations have been produced. For example, the H.235 has been investigated, their calculations updated, and it is currently regarded as the most recent and effective system for security of the VoIP system.

Another method for battling issues and concerns, and one that is the most proficient due to bigger budgets than non-profits, is VoIP being utilized in new structures and the IT work force. Fortunately, the expanding interest of VoIP has guaranteed and emphasized the requirement for more research to build up the effective security structures and countermeasures of CIA threats.

This investigation examines the methods by which such security issues concerning VoIP can be set out to give an apropriate, secure and effective method for correspondence and data trade. In this postulation, the analyst will profoundly examine the relief of VoIP security issues.

Keywords: Protocol adaptation, Network link emulation

Table of Contents

LIST OF FIGURES

Chapter 1

Introduction

Voice over Internet Protocol (VoIP) happens to be the most commonly used service across the globe. It is the transfer of voice messages by using the Internet Protocol. It is an efficient means of data transfer and holds huge importance in the communications as well as the business sector. With the passage of time, more and more applications are being introduced worldwide that make use of the VoIP. It is not only used by the corporate and business sector, but the commercial needs are also increasingly depending upon VoIP. This provides a chance of revolutionizing communication and making the field of telecommunication much more advanced as has been observed in the last few years (Mohammed, Ali, & Mohammed 2013). Some platform and programs have come up to improve the basic structure of VoIP that is currently in use.

The efficiency of voice calls by using the IP has become more interesting with time and is providing ease to people in all aspects of their communications and data transfer. This requires the presence of compatible hardware and software on both ends of the communication. The initial days of voice calls required proper setups, speakers, cameras. Whereas, with the passage of time, this has been reduced to the need of a proper device equipped with all the necessities is enough to get all communications through. Major software fronts are increasingly updating their servers to include the best software and programs for providing easy data transfer measures.

There are some advantages associated with VoIP; the most pronounced of these benefits is the possible reduction in costs of communications. Majority of the VoIP software and call services are increasingly moving towards free call services. People worldwide to enhance their communication experience without any worry about increasing costs are

utilizing some platforms. This is causing rapid adoption of Internet-based calls to avoid higher costs of the regular costs.

Another great benefit of VoIP is the ease of use for all sorts of communication, without any boundaries and problems of location given that a sound Internet connection is present (Castellanos-Lopez et al., 2014). These benefits and the increasing popularity of the VoIP has invoked an interest among the researchers and academicians to learn more about IP and search for methods to further enhance the experience of all users.

Along with the benefits and the increasing popularity of VoIP, there exist security concern and threats that need to be looked into and resolves. Cutting down the security concerns related to VoIP is the need of time. As many organizations and firms are widely using VoIP for reducing costs and increasing the efficiency of data transfer, it is necessary to make sure that the data is safe and secure.

The security threats are a major concern because of the increasing dependency on IP networks for data sharing and transfers. It is necessary to focus research towards not only the betterment of networks but also towards securing these networks. The security threats range from the interception of data by people for whom it is not meant (De Rango, Fazio, Scarcello, & Conte, 2014). Moreover, important information such as security keys, passwords or account numbers might be hacked or misused. This requires an identification of the existing gaps that cause the security lapse.

Server crashes and problems with equipment are among the leading causes of threats as these influence attacks from unwanted sources. Security concerns exist not only for the big firms but also for the personal communications and socializing (Azfar, Choo, & Liu, 2014). Hence security crashes and lapses should be tackled in ways that can be incorporated by people using VoIP for their communication so that a safe and secure IP can be set up and maintained easily.

The basic main problem of the following research is to determine the level of threats and other issues experienced by the non-profit organizations while implementing the VoIP

communication in their system of operations. This main problem was observed in the non-profit organizations because they were receiving threats from their donors to not to implement the VoIP communication in their system as it will record the important and valuable information of the donors' bank account and the cash balance; and the donors will be exposed to the general public.

The developed VoIP implementations that are required by the non-profit organizations are attaining cost efficiency with minimal capital expenditure; easy in adaptation of VoIP services; and, providing the desired security to the communication processes carried out in the non-profit organizations. For attaining such research goal, the following research objectives are specified:

- Identification of existing security threats with the use of VoIP networks. The biggest concern in this regard regards Confidentiality, Integrity, and Availability, which is abbreviated as CIA. These features are the major points of concerns and the leak of any confidential information about a company due to a failure in the integrity or lack of the availability of security measures can be a big threat to security.

- Recommend measures that can help protect data. Moreover, this study will be providing an analysis of crucial steps that should be taken to make sure that business and big firms do not face any loss. Implementation of these preventive measures is the basic step in minimization of the security threats related to VoIP networks.

1.1 Research Questions

In this thesis, the best practices for securing the VoIP communications for non-profit organizations will be explained by answering the following questions:

• What are the most immediate measures that can be taken to solve the VoIP security threats?

• What are the potential unexplored security Threats against VoIP networks regarding CIA (Confidentiality, Integrity, and Availability)?

• How can these threats be averted or resolved with the existing security and privacy mechanisms and what are their shortcomings?

• What are the practices that need to be followed by an entity (Employer or employee, Producer or Consumer, Company or Customer, etc.) to implement a more secure VoIP network connection?

• What are the new countermeasures that can be designed to prevent or eliminate these threats?

This thesis provides efficacious solutions to the network security threats and maintains a good level of privacy of all sorts of interactions that happen over the IP systems. Since VoIP is the most important platform of modern communication and business, this study holds great significance. The major areas of contribution that this study aims to provide are the betterment of the networks regarding security for the operations performed in the non-profit organizations.

This study will help in minimizing the threats posed by cybercrime and the theft of data in the non-profit organizations. This is not only beneficial for the business and firms but also for all personal and social interactions that are now increasingly moving towards VoIP.

Chapter 2

Literature Review

Voice over Internet convention (VoIP) makes it feasible for individuals to convey communication over the Internet. These methods for interchanges incorporate voice calls, video, and sound visits. There has been a striking increment in the utilization of VoIP in the previous couple of years and the innovation being used has additionally been moved up to an immense degree. The cutting-edge period has made it feasible for individuals to move far from the customary calls and settle on web-based calls. An ever-increasing number of clients are moving towards applications like Viber, Skype, Google Voice, IMO, WhatsAp and different methods for Internet-based calls. This is for the most part ascribed to the decrease in expenses related with correspondence through customary calls. The use of VoIP services has made it easier for families to communicate at very cheap costs, the essential requirement is a sound web association alongside the fundamental programming and appropriate frameworks (Assem et al., 2013).

The more up-to-date techniques for interchanges have demonstrated an indispensable piece of interfacing with others, and VoIP has been picking up an incredible favorable position as a correspondence framework and the electronic frameworks are effectively occupying towards these excellent multi-work frameworks (Singh et al., 2014). Likewise, VoIP is believed to be a vastly improved protest for encryption and anchoring data. The sound, video, pictures and all reports can be anchored by means of a legitimate VoIP.

Another fascination is the ability to make video calls, exchange of files and documents during the conversation. The advancement in the use of technology had made it easier for people to carry out their assignments with ease. Aside the normal usage of VOIP in day-

to-day communication, the technology has revolutionized various fields such as telecommunication and medicine.

Patients living in remote places are now gaining from this massive innovation by having access to expert doctors in the city through the use of video conferencing. Data transfer are being done with efficiency since the inception of VoIP technology and communicating with loved ones are easily established with the use of VoIP based technologies and applications (Lamba and Kaur, 2014). Uses of VoIP technology has been adopted in areas such as defense, medicine and secure systems.

The current Internet is designed into multiple layers to ensure proper transfer of information from the sender to the receiver. The transfer of information between sender and receiver is encrypted before being sent to ensure confidentiality. The current Internet model has the following layers below:

- The application layer: this layer contains set of regulations that controls the end goal of a message). This layer also that provides services to the user. Application layer uses the following protocols SMTP, HTTP and IMAP

- Transport layer: this layer is responsible for end to end communication over a network.

- Network layer: this layer operates at level 3 of the OSI model and provides a physical connection between hosts in a network environment. Provision of routing services where data is transferred in form of packets also operates in this layer.

- Data link layer: this is a layer 2 in the stack of the OSI model of computer networking. Data link layer moves data between the network nodes in a WAN or LAN.

- Physical layer: This layer only provides physical connectivity in the OSI stack. This layer also provides electrical and physical specifications for devices

2.1 The Current Voice Communication Systems

The spin around voice calls has been intensifies by the emergence of VoIP technology. The current services used for voice communication encompass mobile operators, telephones and any other related technology. A circuit switching system program gives a bidirectional connection for voice communications. This current system gives users a permanent bandwidth, which ensures a minimal delay in connection. It is a fairly straightforward algorithm with very simple encoding that enhances an improved service. (Aliwi et al., 2013).

However, the Internet protocols use the principle of packet-switched algorithm that purely relied on reduction of data into chunks i.e. packets before transferring to the destination. This principle is ideal for documents and non-voice data but not suitable for transferring voice data. It is worthwhile to mention that this was the main reason for why VoIP was developed. Efforts are continuously being made on the VoIP services to minimize the issues related to jam in voice transfer as well as improving voice quality and communication.

2.2 The H.323

The H.323 is a widely used and recommended protocol in telecommunication networks. This protocol is an entire set of agreement that comprised of transferring of data, videos and VoIP. Its application cut across a wide area such as security of communication, video and audio calls, single point communication and conference call support.

Moreover, H.323 is equipped with modern security techniques such as identification and authorization. It is very secure during communication and it has capability to identify unknown caller by recording all the calls. These features are also useful during incident investigation whereby there is need to track or play back calls to support authority evidence (Shen et al., 2016).

2.3 Session Initiation Protocol (SIP)

Nowadays, SIP has become popular within many organisations and service providers (SP). SP are now switching to SIP because it is lots cheaper and also it has become major way of transport via VOIP. SIP uses algorithm that is very efficient for sending and receiving voice messages and instant messages (IM). It is pertinent to ensure that different applications make use of different SIP support for the purpose of handling smooth operations. SIP make use of port 5060 for its application, and it is important to ensure no stacking of operations is being done (Acharya et al,.2008).

The continual rise in the SIP services has paved way for the development of systems that are capable of supporting multiple applications to be running concurrently without being burden with too many tasks. Having said that, it is therefore imperative to have system that will be able to employ SIP with a dedicated framework for VoIP application. Similarly, telecommunication industries have seen the competitiveness in both the SIP and H.323 networks. The latter networks come with a security support of H.235, which is an interesting approach to the development of VoIP security. This support provides layers of security for protecting data exchanges between two parties (Zhang, Tang, & Zhu, 2016).

2.4 Academic research in VoIP

A great deal of academic research has been directed towards VoIP. The advancements in technology and the idea of revolutionizing human communications over long distance have made researchers more interested in investing their energies towards finding ways to improve the existing systems. Many of the experts in the field of telecommunications have changed gears and are trying to play their role in designing the newer and better means of communications. There have been many designs and protocols that have been proposed by engineering students as a part of their academic projects or due to their interest in the field. Since the ease of communication is of interest to one and all, it is not out of the ordinary to see so much of efforts put in by different people to upgrade the existing systems.

The fields of business and telecommunications essentially require web-based services and VoIP have become popular in very short time. Also, the field of telemedicine is

increasingly exploring VoIP to enhance the healthcare experience for people in rural areas. The use of compressed data packets helps in sharing reports with experts, and the VoIP based calls can be utilized to make sure that the patients get access to doctors without the need of having to travel to different areas to seek health care. This has further increased the interest of people of different fields in VoIP. Therefore, the research interest has rapidly increased in this field and also enhanced the rising popularity of IP based calls and data sharing. Many protocols are being designed to enable data sharing and transfer quickly and efficiently. The business also requires the web-based services for effective communication and data sharing. All these measures have made it necessary for researchers to indulge in research for the development of newer VoIP protocols.

2.5 Voice Optimization

Advancements in VoIP include voice optimization. The data transfer occurs in the form of packets that follow the Internet protocol and format. The performance of this VoIP can be enhanced using various optimizations. One of these optimizations includes the refining of voice quality. The IP defines the voice that is packaged to be transmitted to the receiving end, and only the specific defined get packetized and transferred on the selected network. All other formats are then disregarded. This ensures quality and the selected optimizations are hence put to work. The step of voice refining has made VoIP very popular, and the problem of faulty voices or problems in clear voice transmissions can now be cut down to a minimum (Egan et al., 2016). These optimizations have been proposed and tested to make sure that users experience quality service and can enjoy the VoIP voice calls in a quality that is at par with the regular telephonic calls.

The voice quality has proved the major question in switching from telephone analogs to the digitalized VoIP forms. As a general rule, the bandwidth is selected and programmed according to the IP regulations, making the endpoints of the packets a high priority point. Proper management is required to ensure that the refining of voice quality does not in any way result in loss of packets as this will seriously affect the communication or may result in loss of data. Certain tools such as network trace tools or the tools designed by Microsoft can trace packet loss. The Linux operating systems can be used to run these traces optimally (Jung & Manzano, 2014).

The endpoint screening is carried out on the devices where the data is being sent. The usual default parameters have to be upgraded to ensure that all necessary optimizations have been set in place. The performance and voice quality can be enhanced after running careful screens and using newer software tools designed specifically to suit the VoIP systems (Irshad et al., 2015).

2.6 Packet loss Prediction

Identifying the extent of the loss is important to analyze the points of loss and carefully shut those ways off. Various models have been proposed to analyze the loss during VoIP based communications. The most basic way of predicting the lost packets is by using the Fractal prediction model that was proposed way back in 1986 (Carvalho, et al., 2013). This model works on the principle of forming a graph between the various points of communication. This pathway leads to a count of all lost packets, and the final count reveals the total number of lost packets during the transfer (Jiang et al., 2016).

2.7 Covert communication via VoIP

The concept of covert communication is the transfer of secret messages or data via the existing means of communications. VoIP is widely being used in this regard. The major concern was the security of the data being shared. However, the modernizations of the modes of transmission and the various codes, screens, and optimizations have made the VoIP very efficient for transmission of data in a secure way (Dabbebi, 2014). The modern protocols include filters and packet formations such that the data cannot be intercepted or breached by networks that it is not directed to or intended for. Audio, video, text files, images and a lot of other formats can easily be sent and remain secure and hidden from possible threats.

The VoIP provides a means of covering and securing data by utilizing algorithms for steganography (the art of concealing messages). The media streams of VoIP provide ample space and frames for integration of covert channels. These measures ensure that the data is secured by more means that the encryption and end-to-end coding (Mazurczyk, 2013). SIP can be used for this purpose to provide control over the data as it is being shared between the parties involved in the communication.

Some algorithms have been proposed till date to provide a means of carrying out efficient steganography. These algorithms are generally IP based; some of them even work upon the principles of the RTP (real-time transport program). The spatial system has proposed an algorithm that uses the spatial orientations of the data packets to create concealed frames work for keeping the data hidden. This algorithm also ensures that no packet is lost during the transmission and that there is no breach in the security of the data being shared (Huang & Tang, 2016).

Among the many protocols in use up till now, there is also the proposal of using the lost packet network known as the Lost Audio Packets protocol of Steganography. This protocol makes use of the information that is delayed to create a framework of security by creating a separate storage space. This algorithm can greatly enhance the capacity of the data that can be stored and secured during the VoIP based sessions (Huang, Tang, & Zhang, 2011).

2.8 Benefits of VoIP

Quite some benefits are associated with VoIP. These benefits include but are not limited to reduced costs of communications, a higher degree of reliability, ease of carrying out other tasks and sharing of materials and documents at the same time. A good network ensures that the connection remains intact and that data can be transferred without any hindrance.

The incorporation of VoIP has revolutionized communications. It is now possible that the normal phone calls be linked to the Internet using an interface device that can be used to convert the signals of the phone into a digital signal that can then be used via Internet communications. The VoIP has made it possible to convert a normal call to an Internet based call. This has to be tested for efficient working in a manner that is different from the regular PSTN system (Liu et al., 2015).

Reduction of costs and ease of communications are backed by the portability of devices that has been possible due to the integration of VoIP. There is also a great deal of flexibility that lies in using VoIP for all sorts of communications. Since Internet usage has become common, more and more people are now diverting towards VoIP based

communication to maximize their gains at the lowest possible costs. Not only individuals but also large firms are moving towards VoIP based communication due to the ease, low cost and security of data. Even the transfer of files is now rare in the hard copy format. Professionals make use of the VoIP based communication for all sorts of file transfers and sharing of data.

The most remarkable feature of VoIP communication is the removal of all barriers and boundaries that exist in the regular cellular networks. One is not bounded geographically when using the VoIP system for their daily communications. In the regular networks, one has to change their card or number as per their geographical location. Whereas the VoIP based communication is devoid of any such need and only requires an Internet connection to work, without the need to change any of your details. Plus, it also supports the older forms of technology. Proper configuration can also lead to the provision of access to the fax machines of the previous decades (Li, Mao, and Rexford, 2012).

2.9 Shortcomings

Some shortcoming and concerns have risen regarding the use VoIP. These concerns are majorly about the security and safety of connections and the data shared. There are concerns about social threats that is the security of the people. The users are concerned about the presence of their data on the Internet sources. There are common incidences of bugs, security breaches, viruses that destroy one's system and theft of data by hackers. Such negative experiences by many in the past have raised concerns and made people conscious about their usage of the Internet sources for communication (Rathore et al., 2016). Regarding security threats, the communications can be eavesdropped on, the safety of people can hence be threatened by their personal and private information being leaked to the wrongdoers and misconducting mischief who take pride in being efficient hackers.

These threats are also posted towards law enforcing agencies, whose calls might be intercepted and overheard through security breaches by unauthorized people who break into the connections and eavesdrop on the VoIP sessions without being detected or recognized. Denying the occurrence of such breaches is to fool oneself since such

incidences have been occurring since the very beginning of the Internet era. Along with programmers, the hackers have also become quite popular (Gruber et al., 2015). There have been security breaches on many occasions, and these breaks insecurity can come from tampering with the hardware or somehow manipulating the software being used.

2.10 Social threats

Social threats are the major concern of using VoIP. It is extremely important to ensure that the networks are secure and the calls are verified and authentic. Many incidences of proxies have come up which have given rise to concerns about security (Ben et al., 2016). Proper protocols need to be developed and are constantly being searched. These protocols should ensure network safety and authentication of the personnel involved at both ends.

2.11 Other Weaknesses

Understanding the existing weakness of the system requires an understanding of the system itself. The VoIP makes use of the Internet protocol (IP) as its backbone. This is where the most basic weakness can arise from. Among the various existing problems, there is a chance of resource exhaustion. This can result from attacks by unauthorized users that create a shortage of available IP addresses and may result in causing a burden on the memory and bandwidth. Too many requests and calls at the same time might result in the exhaustion of resources and the network, which may end up causing a shutdown of the application and pose problems for all authorized users.

2.12 Security measures

Security measures for VoIP networks are created to ensure proper authorization of personnel using the VoIP networks. It has to be made sure that there is no breach of privacy and that unauthorized users do not manipulate the systems. The authentication steps can be carried out at various levels. It can either be during the configuration that occurs at the time of authorizing a new user or at a step later. Once this authentication step is done, the equipment is now set for the user to make use of a server securely. The customer premise equipment (CPE) exchanges a network authentication key with the server. The network server, in turn, sends back an encrypted key. Some security protocols are being used widely. These protocols include File Transfer Protocol (FTP), Session

Security Layer (SSL), Trivial FTP, Transport Layer Security (TLS) and Secure HyperText TP (Ghafarian et al., 2007). These security measures help in proper trafficking of voice signals and their separation from other data signals during the transfer.

Apart from the authentication, another measure is the establishment of Security Association (SA). This is a virtual connection that is established between different devices. There is an exchange of security keys, certificate or other encryption between these devices after the connection is in place (Zhang, Tang & Cai, 2014). This step has to be carried out during the time of establishing the connection because it is a lengthy process and may hinder with the signal transmission if left for later stages. There is a time lapse of about 2-10 seconds taken for the establishment of SA.

2.13 Securing the Packet exchange

The packet exchange during the VoIP based calls; there is a problem of security. The conversion of ordinary calls to the digital Internet-based calls requires an analog-digital converter. There is also need to compress the voice data to make the transfer easy and efficient. Hence, the signals are cut into small data packets that are subsequently transferred from one device to another in the form of a voice call. This particular step is where the packet security system comes in action. These packets of signals are secured and are not established separately for each call, rather the establishment occurs at the step of network configuration and the same remains intact for future use. This is due to the reason that separate security setups for each call would have resulted in delays and possible security lapses during the delays.

2.14 Challenges for service providers

The network service providers face a huge number of challenges regarding providing secure networks to all users. These troubles arise from the generation of a pathway to transfer data packets across the network safely and securely. The infrastructure of packet data transfer has to be made secure for the customers. The security companies use a firewall that is constantly under threat of security breaches because this proves as the first defense mechanism towards forged utilization of the network. Hence, this particular step is the first and foremost target for attack.

Securing these networks using specifying particular IP phones cannot be considered in this modern era of constantly upgrading technology. Such measures would result in limiting the choices for customers and hence prove a failure in the long run. One major problem with the IP phones is their openly accessed location and exposure of data. This proves as the major threat to security and needs the utmost attention from service providers. Secure transfer of data through the VoIP networks needs to be ensured (Liu, et al., 2013). All network service providers have to make sure that the infrastructure used holds enough space to accommodate the advancements and deliver the best service for easy VoIP data transfer in a secure manner.

2.15 The biggest barrier

The biggest barrier towards providing a secure network lies in the fact that the traditional security measures such as the firewall systems and other such components that are used for securing networks cannot be implemented directly to VoIP. Here, a different and additional layer of security is required. This additional layer is based on encryption of the signal packets such that they are secured at the IP layer using IPSec or at the second stage, which is the application layer. This ensures that access is not granted to unauthorized users (Antwi-Boasiako et al., 2016). To all such users, these packets will be in a language that does not make sense.

Secure implementation of VoIP requires setting proper guidelines and ensuring that these guidelines are followed and constantly upgraded and refined to prevent security breaches. Some key steps include modification of the existing security systems. Along with this, the network providers must use separate networks for voice and the other data. Very strong systems should be developed and implemented to secure the entire process from the established connection to the transfer of data. Authentication should be strong, and encryption should be set for ensuring protection. The gateway systems should also use good encryption and strong codes for security (Wahab et al., 2013). All these measures can be backed by making sure that VoIP transfers are avoided through the regular firewall systems.

Many other systems can be utilized for VoIP traffic. These systems can either be dependent on particular protocols or may even be independent; examples include the

ALGs systems specific for VoIP. Also, there exist filters that can rule out any data packets that are not part of the regular system or pose potential security breach. Management of the network should not in any way be manual; the automatic system should be incorporated and strengthened. Tunnel mode of the IPSec should be used for all sorts of voice transport to maximize the security as this system tunnels and masks the IP addresses and secures all data being transferred.

2.16 Future Perspectives

The future perspective is quite bright for VoIP since so many algorithms are continuously being proposed and the previous ones are regularly being upgraded. A great scope lies in making use of VoIP for various other purposes. One of the most beneficial uses of VoIP is in providing ease to those in remote areas using introducing technology-based care and making it possible for them to seek healthcare from the experts based in the urbanized areas. The basic algorithms used for VoIP are now also being used for telemedicine, and there is a great scope of making it bigger and better (Scholl, Lambrinos, & Lindgren 2009). The security breaches can also be overcome with dedicated research and building better algorithms by refining the transmission of the packet data. Once the security concerns over the Internet based sources are covered, there will be better use and more popularity of VoIP. The various patents and proposals that are working up till now are also being refined and will surely be made better in the future to keep its pace matched with the rapidly changing technology and devices.

Chapter 3

Threats to VoIP networks

The rapid increase in the use of technology and the adaptation of the modern world towards the technological advancements are leading towards a revolution, which is larger than anything human history has ever experienced before. Increasing amounts of techniques and equipment in the field of telecommunications and computing have strengthened business, firms, institutes and also education. This has caused adaptation among the masses towards the newer technologies. Better equipment, latest hardware, upgraded software are constantly causing an uproar and people seem to be in a competition to move faster towards what is better. In this struggle of upgrading, systems are also constantly leaning towards the increased amount of threats. Security concerns have escalated a great deal in the last few years. The move of information from hard copy files to soft copy has made information more and more vulnerable to theft and misuse (Liyanage et al., 2017). Owing to these security concerns, the security experts are in a constant search for combating threats and fighting off unwanted bugs and access of unwanted personnel.

The Voice over Internet Protocol (VoIP) is not only concerned with the exchange of information and voice calls. Advancements have made it possible for video chats to be included in the VoIP services, making communication more flexible and apparently much smoother. These benefits have made it more popular, and a large amount of work goes into refining the services for better experiences (Khan, 2016). Also, security threats escalate which have to be tackled with the advent of every new software and possible VoIP related hardware.

Threats associated with VoIP networks have been explored, but there are still unforeseen situations that may arise and require newer and better measures of data protection. Some of the most pronounced areas of threats are the social threats that are aimed at bullying people by gaining uninvited access to their data, threats of eavesdroppers who might simply be taking undue advantage of someone else's data (Keromytis, 2009). The other types of threats include those that arise due to problems with the server or the software. There is also a chance of one's data becoming inaccessible due to unidentified breakdown or problems with the network (Keromytis, 2009). These are all among the concerns of VoIP usage and have to be sorted to provide all users with experience and uninterrupted data sharing and communications.

Moreover, these threats have been categorized as CIA threats, i.e., Confidentiality, Integrity, and Availability. These important features determine the types of threats and also the loss that can be faced by users owing to these threats. Security concerns and data loss are among the most pronounced threats facing the modern world. People have their crucial information and data sharing through IP networks (Chakraborty et al., 2016). Additionally, the data sharing of large and small firms, exchange of crucial information about services, accounts, and dealings are all carried by the Internet protocols. Important data sharing and meetings are also being carried out using the VoIP (Boehmer, 2013). Here, the threat of unwanted eavesdropping is also a major concern. Hence, all protocols have to be analyzed to prevent any loss that can create problems for users.

Security and confidentiality of information over the computer-based systems are one of the biggest threats that revolve around the usage of VoIP. Security measures are required to eliminate these threats. Confidentiality threats are the biggest concerns, and crucial and classified information should not be exploited or misused. To ensure that information is only accessed by reaches people that it is meant to reach. The infrastructure has to be maintained as to make sure that the vulnerabilities are fixed, and bugs are warded off (Deshmukh & Devadkar, 2015).

Many of the confidentiality vulnerabilities are similar to those problems faced by the regular telephone usage. These issues include interception of VoIP based calls and

recording or extraction of crucial information that is being exchanged. This is similar to telephone call taping and eavesdropping over the phone lines. Unwanted personal, hackers or a potential attacker may make use of the same basic tactics and gain access to VoIP calls and data exchange (Shamsolmoali et al., 2016). This may lead to a loss for the users regarding classified information being leaked and in case of big firms or business, classified information may be threatened or may even fall into the wrong hands.

The confidentiality threats can be due to shortcomings in the network, or it can also be the deliberate attempt of unauthorized users to gain access to the network or to eavesdrop the important business dealings and calls. There can be a security breach in the system that may go unidentified and lead to loss of important data. These threats to confidentiality are the major liability in the use of VoIP and may be the major reason behind security concerns of firms using the Internet protocol based calls and information exchange.

3.1 Integrity Threats

Integrity threats are related to the changes and modifications made to the data being transferred by unauthorized personnel. It is important to maintain the integrity of VoIP and make sure that the voice packets are prevented from unnecessary changes made by those who were not meant to have access to the data. Unauthorized activities come from the breaches in passwords and codes. Other attacks that can make the integrity of VoIP questionable include decline in quality, problems in getting connections through and hijacking of sessions by unauthorized users. These threats loom large, and with the increase in the number of software and hardware devices that are used for voice calls using IP, there has been a remarkable increase in the number of threats that are faced by users regarding VoIP integrity. Despite proper formulation of caller IDs and setting passwords, security breaches are common. There is even the threat of system crashes due to unwanted attacks and bugs.

The loss of packets also comes under the integrity threats and has to be countered accordingly. The loss of important data during transfer through VoIP is a problem that as to be tackled. It has the potential of ruining connections and making the users face problems and have a bad experience in case of important business transfers. VoIP

networks are not only used for the voice calls but are also many times equipped with data sharing options. Any loss of these data packets can be a major blow to the communications. Unauthorized personnel can also breach the highly classified communications as a result of bugs in the line and loss of packets from the main source. Also, the compression and decompression steps may have certain liabilities and the integrity of the network may be compromised which can lead to loss of data and also problems with availability can stem from here, leading to an overall bad experience in the use of VoIP networks (Dabbebi, et al., 2014).

3.2 Availability Threats

Availability threats refer to the denial of service, which can lead to interruptions in calls or data transfer. The call networks are adversely affected due to the breaks in service. Unavailability can seriously cause a decline in the number of users on the network if the interruptions continue for long. Another possibility is that the denial of service is occurring due to unwanted interruptions by unauthorized sources. There might be those who buy the lines or connections to disturb the online experiences of others (Rathee et al., 2015). Such threats come under availability threats and may severely ruin the experience of people who constantly have to face a breakdown or interruptions in the voice calls due to network unavailability.

Spam and system bugs can also cause a threat to network availability. The overall service decline can be related to a class of the firewall or spam-filled servers. These cause delay in the establishment of connections and transfer of voice packets. The overall bandwidth required for setting up a connection can be causing a burden to the network due to firewall crashes and spam (Bilski, 2014). There are thorough actions required to ensure that the presence of unwanted spam does not cause questionable availability of VoIP network.

The denial of service attacks can be a very serious threat in case of emergencies. Since the majority of the personal and professional communications are now dependent upon the Internet protocol based calls, unavailability of service may lead to the emergency situation becoming more of havoc. This may be due to the DoS attacks, or there is also a chance of physical barriers being set to interrupt someone's sessions. Flooding of the network with too much of unwanted data packets may result in clogging of the network

and result in an inability of the network to keep the connection running smoothly. On the other hand, the denial of service can also be due to unforeseen causes such as unavailability of the network due to bad weather influence or breakdown of main supply (Stelkens-Kobsch et al., 2015). There can also be an exhaustion of network due to too many users and subscribers at once.

3.3 Other threats

Threats associated with usage of VoIP for Internet-based calls may seem charming because of the cost reduction. But the threats are too many and undeniable. Threats other than the very basic CIA threats include the overall security threat, bugging, eavesdropping, loss of important data and other social threats (Gilmore, 2015). The social threats affect people on a personal level. Your calls and sessions may be intercepted by the wrong people and even recorded to be used against you. The bugging techniques can lead to lose one's important data or make one's system crash. This again revolves around the basic CIA threats, but since the VoIP is common and is in use by people in their communications, it is necessary to look deeper into the social aspects of these threats. Unlawful access to someone's call sessions is a major threat to one's social connections and at times also reputation (Satapathy & Livingston, 2016).

The threats exist and keep increasing due to the increase in the net number of users and the widespread reliance of business on the VoIP networks and other Internet protocols. The employees might be proving as a source of the leak and may be causing the spread of information to outward sources and unauthorized personnel. Corrupted nodes, denial of service and the overall network load is generally due to unauthorized personnel having access to secure networks. This access can be attributed to breach in the information of ID and secure lines; the passwords may have reached the wrong hands and hence spread from there. Inappropriate use of services and physical attack onto the devices and software is among the biggest issues that have to be tackled. These threats are looming large on the VoIP services and are leading to increasing concerns about security. Social threats are increasingly becoming a problem as many rivalries and increasingly resulting in people accessing data in an unauthorized way to get even with people they consider as

enemies. This is not only unethical but also very disturbing as the personal and private information of people can be used in negative ways to make people's lives miserable.

3.4 Insider threats

The insider threats are those, which are from the company itself and these, are totally unlawful and can have very severe decline the security of the important information of the company. The competitive business faces many issues and in case of any problem by the employee or due to some accidental reveal of the important information's and passwords to the potentially not trust worthy employees, this can be a major blow to the information and document of the company. This risk is one of the biggest and most critical one as all other issues stem from here and if it is not tackled in time, this can grow bigger is size and can have more problems in future. Those companies, which rely on VoIP are majorly are risk of the breaches and these risks are unlawful and also questionable. Companies that rely on VoIP are largely at risk of breaches. These insider threats are unlawful and questionable (Smith, 2015). They should be analyzed on a regular basis. Those who deliberately cause security breaches should be identified and held accountable.

Overall, it can be said that there are too many existing threats that can mar the popularity of VoIP. Users may face trouble in getting their calls through due to the high number of subscribers who might be causing a network jam. The CIA threats are increasingly causing threats among the big firms and businesses that need to find a way to securing their connections and maintaining the integrity of their communications. A large number of security threats can be a problem for not only the professional but also personal communications (Patel & Buddhdev, 2013). These threats have to be warded off along with the refinements and up gradations of the networks to strengthen the networks and make sure everything continues to run smoothly.

3.5 Threats from humans

These mostly have their focus on human kind of error in the configuration file, some kind of mismatch of protocols threats from some unknown identity. Some of the most common

types of threats will be phishing, theft of service or some unwanted contact. (Jayaprakash, 2012)

3.6 VOIP Call alteration threats

In this kind of risk, there is situation of some unwanted user who is trying to make a hidden link or connection in the conversation, changes the content of the call and he also himself ensure that nobody will capture him. (Callegari, 2009)

3.7 Denial of service threats

It refers to the term of flooding in the traffic of communication. In some cases of the VoIP is someone comes between any conversation then this kind of attack is very crucial which stops up losing some of secret information and this can be unmanageable by the company to face it. (Callegari, 2009)

3.8 Service abuse threat

These problems refer to some kind of misuse of the service of VoIP such as nonpayment and some frauds of billing. (Jayaprakash, 2012)

3.9 Physical Access Threat

This threat is also one of the biggest threats that are really not bearable in which somebody comes in the environment physically and he destroys the physical network. This is the highest kind of lacking in the level of security. (Jayaprakash, 2012)

3.10 Interruption of services threats

These kinds of risk come when there is something going on which was not expected and suddenly blocks all of the services of VoIP such as weather, natural disaster or sometimes the failure of the services like power which may have resulted in affecting the quality of the service such as quality of calls. (Shan, 2009)

3.11 Transmission issues

Unlike POTS, which is known as plain old telephone service the system of VoIP, rely on the packet switched telephone for sending and receiving the message. Instead of making the dedicated channel between the two end points for the time of the call by the use of copper wire and analog voice information, the data of call is then transfer by the use of many packets individually. By using these packets, it is much possible for quickly sending and having the voice data over the Internet connection and the technologies of VoIP are designed like which these packets are re ordered at their destination, so these calls are not out of the sync. Risk is the transmission medium itself and the POTS lines are normally secure as a single and dedicated connection is only the point of contact that is between two telephones. As when the data of voice is transmitted over the Internet at large, to becomes the possible for some malicious actors for sniffing out the traffic and either listen in on the conversations or stealing some of the main pieces of the data. The solution of this problem is that the data should be encrypted before it leaves the local servers and one have two choices in which one is to set up his or her own encryption protocols in house or opt for the vendor of VoIP which bundles some private network which is able to make the secure channel between his employees and whoever they call (Lazzez, 2014).

3.12 Denial of service

One more risk of security inherent to the VoIP is the denial of service. The attacks normally intended to make the voice network slow and shout down for some time. It has been noted by SANS institute whitepaper that the malicious attacks on the system of VoIP can happen in many different ways in which the first one is like the network may be targeted by the denial of service DoS flood that overwhelms the system. In this situation, the hackers may also choose for buffering the overflow attacks or infect the system with the worms and viruses in attempting for causing the damage or trying for preventing one's system from being accessed. It also has been noted by the recent article of CBR that the attacks of VoIP are becoming much popular avenue for the malicious actor. UK based institute said that with less minutes of bringing the new VoIP service online, the attacks volumes increased a lot (CERN, 2015).

If one deals with these attacks, it means that he or she is undertaking the audit of security of one's network before the addition of VoIP. Looking for the insecure endpoints, the

third-party applications and the physical devices, which may serve as the jumping off points for the hackers for finding their new way into one's system. This time is very good for accessing the legacy applications and older hardware for the determination of they are able for handling the requirements of security of the Internet-based telephony. It is also worth of taking a good look at any kind of network protection protocols and firewalls for the determination if changes have to be made.

3.13 Eavesdropping

One more issue for the systems of VoIP is eavesdropping. In this situation, if one's traffic is sent which is not encrypted such as it is possible for the motivate attackers to listen on any call made then the same go to the former employee who have not been properly removed from the system of VoIP or he may have their login revoked (Niccolini, 2006).

This kind of threat allows the malicious actors for stealing the information, which has the inclusion of the phone numbers, PINS and also the personal data of users. Impersonation is also possible in this situation in which hackers are able to leverage the VoIP system for making calls and pose as the member of one's company. In the case of worst the customers and partners can also be tricked into handling over the confidential information. Developing policies is connected with handling this kind of threat that speaks to the nature of the issue and the departments of IT should regularly review who has the access to the system of VoIP and how far this access extends.

3.14 Vishing

As per the Canada government "get the cyber safe" website is one more emerging threat to VoIP is the voice phishing and vishing which occurs when there is any malicious actors who redirect the legitimate calls to or from the VoIP system and instead connect them to the online predators. From the perspective of an employee or the customer, the calls may seem to be legitimate and they may also be convinced for giving the credit card or other kind of information. SPIT which is known as spam over Internet telephony is also increasing the issue in which the attackers are using the network for sending many of the voice messages to the un suspecting phone number which is able to damage the reputation

and consuming the transmission of VoIP capacity (Butcher 2007). For managing this, one should consider the installation of separate and dedicated Internet connection only the VoIP system which allows monitoring the traffic in easy way.

3.15 Call fraud

One last major issue associated with VoIP comes from the call fraud, which is also known as toll fraud. This happens when the hackers leverage one's network for making the large volume and lengthy calls to the long distance of premium numbers, which results in the massive costs to one's company. In cases of this kind of problem, calls are mostly placing to the revenue generating numbers like international call numbers, which are able for making the attackers, and leave one with the bill. (Park, 2008).

Chapter 4

Countermeasures for threats faced by VoIP Networks

Countermeasures for confidentiality threats are an absolute necessity, as users need to have their data protected and secured from all misuse. Many protocols have been proposed for maintaining confidentiality over VoIP. Caliskan and Pterson (2013), proposed a dependability method that includes security measures for confidentiality, availability as well as integrity. The basic outline of the algorithm is managing the resources to not burden the network with too much of data packets. The system works fine in a well-defined state, but upon the identification of data load, the system lowers its efficiency so that some of the applications become unavailable (Çalışkan and Peterson, 2013). This helps in ensuring that too much of data is not trafficked at once, this is also crucial for preventing theft of data. Certain parameters have been incorporated into this algorithm which ensures that the system is rejuvenated and activated when deemed fit or when the threat is detected to have ended or passed.

Another countermeasure has been proposed by Khan, M (2013), which includes using an Audio Secret Sharing algorithm that can be joined with VoIP to maintain the network security and confidentiality. Some cryptographic techniques have been incorporated in this algorithm to secure the secret sharing. Also, a multipath routing technique is used to ensure that data packets are not jammed or misused during transfer. The messages being shared are encrypted in this algorithm, and an end-to-end encryption ensures that the security is maximized. The simplest and probably easiest way of securing the data and managing VoIP based calls without threats to confidentiality include setting up an authentic username and a code or password.

Moreover, there is also the use of a firewall to enhance security. The security of individuals, as well as companies and firms, can be ensured by the implementation of a

securely designed firewall. This is a measure of providing security most simply. Also, the incorporation of firewall can cut down the need for security checks and measures at every step and all ends of the communication. Therefore, a load of too much data and encryption can be lifted off from the main network and the network can be secured. The efficiency of data traffic is also maintained and refined by this step.

4.1 Countermeasures for Integrity Threats

Managing data traffic can curb the integrity threats. Algorithms that manage the data into suitable packet size can be useful in this regard. The best possible countermeasure for integrity threat is the use of well-defined algorithms that can help in curbing the problem that occurs mainly due to heavy traffic of data over the Internet or at times due to too many users on one network. Integrity is usually compromised when there is a high use of data packets, and this can cause a system crash or may even open loopholes for possible security lapses.

One of the proposed methods is the use of the hop-by-hop method, which implies that the data transfer occurs in small packets to make sure the integrity of the overall network is maintained. The network is structured in layers that maximize the security and ensure that everything is not let onto the network at once. Also, multifunctional algorithms and systems can be incorporated into the end-to-end encryption to ensure the integrity and prevent loss of data packets. The secret sharing scheme can also have a very good impact on the security of the VoIP regarding integrity. This scheme makes it possible for users to protect their data and prevent any loss or breach during data sharing. This can be particularly useful regarding dealings with big firms, where a lot of highly classified and confidential information is shared through the voice calls. A breach of security can lead to a loss of business and may create problems in the business-related trust. The speed of sharing is also maintained to prevent the communication network from crashing. A huge load is likely to create many loopholes, which can be curbed by the method of dividing the data into packets and also compressing those packets to transfer data as packets rather than a bulk at once.

4.2 Countermeasures for Availability threats

Availability is a big concern with the VoIP networks as there is an increasing number of users that are rapidly diverting towards Internet protocol based voice calls rather than using the general phone calls. Many of the big firms and business rely on the VoIP networks for their important calls and video conferencing. Hence the security measures have to be well regulated, and the availability has to be ensured to minimize problems and maximize the use without threats or breaches.

The DoS attacks have been explored, and the major reason found to be associated with these attacks is the lack of strong encryption and passwords, which make it easy for unauthorized users to get access to the network. Voice calls are intercepted or breached using such loopholes in security (Schmitt, 2013). The countermeasures for availability problems related to the availability of VoIP have remained unexplored in the past. But the rapid increase in the use of the Internet-based voice calls has led to an increasing interest of researchers and also business firms to invest in search of security measures. Also, the number of users per network has to be managed along with algorithms to protect the networks and limit the access only to the authorized users (Fachkha et al., 2015).

Different simulations can be used such as the dependability method can be used for ensuring that there are no threats to availability. Reliability tests and statistical analysis of the system should be carried out to detect any possible opening for unauthorized users. The overall functioning of the system and network has to be analyzed and scored to help the users detect changes and report problems immediately (Rohloff et al., 2016).

The transport protocols have to be kept in check to maintain availability. The most important countermeasure for cutting down threats to unavailability is to ensure that the transport protocol is incorporated after consideration of the amount of data that is transferred through that network or the bandwidth that is used on an average by the company, firm or an individual. The compression and decompression and the overall use of the network have to be estimated, and the algorithms that can support the usage should be incorporated accordingly. This also helps in ensuring that there is a net amount of

packets always managed and no packet loss occurs that could make the availability and integrity of the VoIP questionable (Soloducha & Raake, 2014).

4.3 Internet-bound VoIP traffic and its countermeasures

Interconnectivity of the telephone traffic over a routing system can be viewed as less secure as compared to the previous methods of telephone networking of circuit switched networks. VoIP traffic occurs when some clients to be served and be given feedback by the server are many, and thus the server becomes overwhelmed in sending all the packets to the required ports at once. This, most of the times leads to processing problems such as reduction in the speed. Common problems that can occur as a result of VoIP traffic included the sound jittering and delayed sound transmission, which can be solved or managed by considering the following remedies (Mazurczyk, 2013). The Figure 1 displays a difference between two communication types where one is with a Quality of Service (QoS) while the other one does not have. It is important to note the Quality of service ensures that the prioritization of various transmissions is done and that all the proper transmission processes are considered.

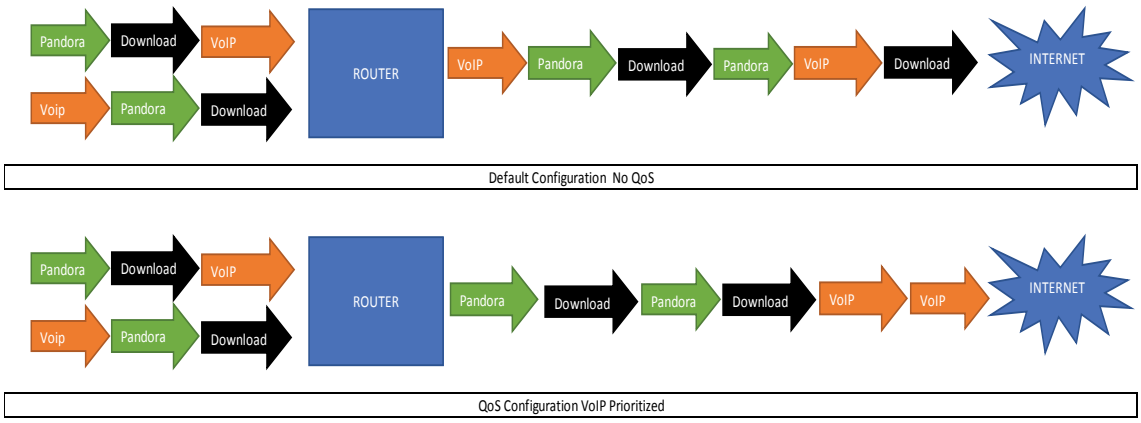

Figure 1: Difference Between Non-Prioritized and VoIP prioritized QoS (Mazurczyk, 2013)

One of the ways with which voice over the Internet protocol traffic issues can be solved is by the server identifying the specific traffic and changing its processing priority on the server so that it is processed faster and considered first in the processing queue. Some programs can be used to calculate the various amount of traffic that a certain packet is

facing thus gives the server a prompt to consider some transmission and give them a higher priority. This is thus prioritizing some delayed and congested VoIP packets in a network environment.

4.4 VPN tunnels

Virtual private networks in a given setup can enhance a different means of improving connectivity of the voice over Internet protocol. This is possible by utilizing the VPN tunnels and using them to network a remote phone with the other phone systems in the corporate offices. This mitigation method is, however, slow and will need some time for setting up the system (roughly 30 sec) and the VPN must always be on and working for the communication to occur.

4.5 Patching challenges and its countermeasures

Most software and running programs in computers and other operational equipment require proper maintenance regarding update and activation to ensure that the programs are properly running and contain the most current capabilities according to the solutions they are supposed to provide. In networking, it is still challenging as patches: the software security update utilities still do not exist for mobile phones and VoIP. Most organizations using voice over the Internet protocol today do not have any downtown windows type to improve and automatically set up VoIP and telephone diagnostics. It is challenging to administrators as they discover that data diagnostics does not work with the voice packets over the networking (Gruber et al., 2015).

4.6 Regularly checking the entire network layout (system preventive maintenance)

Even though, there are no appropriate patches to ensure proper diagnostics and updates for voice over Internet protocol, it is advisable that the administrators who run the various network servers in an organization, for instance, to regularly check the network programs and ensure that preventive maintenance is done regularly by the installation companies or the organization's expert. This will help in preventing future system failures. The organization through the network administrator should also ensure that they have access to the most recent patch management technologies and systems which can identify possible system errors and causes of system failures.

4.7 Data loss in case of a system failure

System failure is inevitable and cannot be predicted. Most systems including the network management systems are prone to breakdown and failure. This can lead to a massive loss of data and information that is very useful to any organization. The voice over Internet protocol is a form of a program that is managed to exchange information and enhance communication. When a network system breaks down or fails, the organization is likely to lose massive data which was not backed up or saved in an alternative source. Voice over Internet protocol program contains information like directories and call histories that provide information of the communication registry; the as well contain peoples' contacts, written messages, some VoIP telephones are as well able to record voice information for future reference. All these are prone to lose if the system backup is not done regularly.

To prevent data loss and improve the data security of an organization using VoIP, there should be a regular back up the process by the administrator to ensure that all the registry, directories and call histories are secured in case of a system failure.

4.8 User and staff ignorance on network security measures

Apart from ensuring that all the security measures are taken, it is important to put into consideration that all the workers within the organization might act as the main loophole to the security of the organization's communication network. The sensitivity of the information being conveyed through the voice over Internet protocol program is sensitive, and unauthorized access can lead to major information security issues to an organization. The staff members can unintentionally provide the network security loopholes to unauthorized users or might plot to destroy the security by knowingly coordinating with outside members who might meet some information about the organization for their own benefit or the downfall of the organization.

To mitigate the security issue of information leakage about the security of a given network, it is important to train the staff on the appropriate measures on what information should be given not to be given or shared with unauthorized users. Most of the time security information about an individual network leaks to the public through ignorance of the staff members thus through staff training, systems security can be enhanced thus more reliable voice over the Internet protocol transmission.

4.9 The use of default gateways and private IP addressing

Alongside the remedies mentioned above, it is advisable to use gateways and private IP addresses when networking any organization or home to enhance the security of the entire network. Just like networked computers, VoIP telephones are as well assigned IP addresses that identify them in a certain network. Within a given network, a router will assign a private IP address with a single gateway address that will enable an exit from the system to the extensive external network. This helps in creating a single out the way with no more ports that provide loopholes to the system. Figure 2 displays a network layout where VoIP telephones are interconnected under one VoIP gateway (Wahab et al., 2013).

In the figure 2. There is a connection within the central room where various VoIP telephones are interconnected from one gateway that acts as a switch as well enhancing private IP issuing and connectivity. This is a secure form of networking since the phones will be assigned private IPs rather public IP addresses that are most of the time not secure. The gateways are connected to an Internet router that connects them to the public networks. The gateways act as outside link in and out of the network. By giving the default gateway to any networked system, the security is enhanced since there will be only one channel in and out of the network. From the above diagram, it is observable that the systems are enclosed, and that access is only allowed through the gateways thus more security. There is a remote user who might act as the server for all the networked devices and can monitor all the clients and respond to their requests.

Just like in any other network, voice over the Internet protocol is only different since the packets shared are informed of voice or videos in rare cases. Another security measure that can be put into consideration alongside the gateways is the use of firewalls. The purpose of firewalls is to filter and lock all the pots out of and into the network this restrict all the downloads and uploads of data packets as well as unauthorized access by the users of the system.

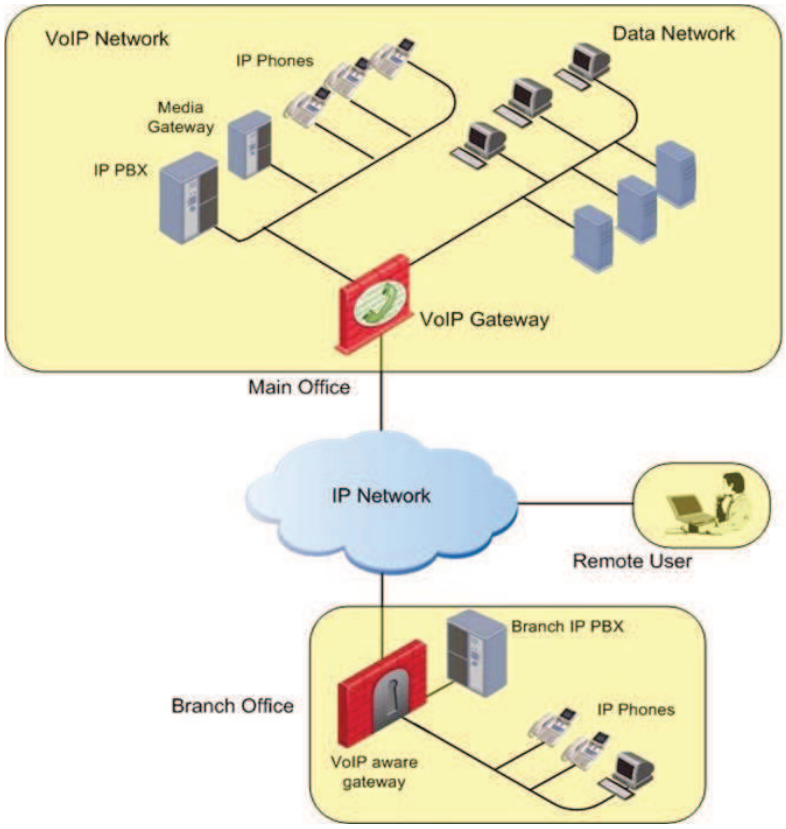

Figure 2: An office layout VoIP network (Wahab et al., 2013)

If all the above-discussed measures are taken into consideration, voice over the Internet protocol can be made more secure and reliable. Regular preventive maintenance of the system and patch updates and diagnostics will enable a proper running of the VoIP system in an organization or a home setup.

The following section is going to describe some of the methods for securing the communication of VoIP by the use of some of the previous research.

4.10 Port Authentication

This kind of work is very much useful way for securing the different communication. This uses the standard such as 802.1 x for confirming the access which is between the user and the authority. This kind of authentication will also be helpful for securing the network. In it, the invader has to authenticate first about him with the central authority after that he will be given the access, which is very much secure. But when the traffic of

VoIP joins with the Internet, then this type of authentication does not work and then it leads to opening the access for all invaders (Butcher, 2007).

4.11 Categorisation of traffic

The work for categorizing is helpful in securing the network as it will divide the traffic into different parts such as voice and data and then it will be useful in securing the network as the traffic divides so the chances for damaging to the communication will decreased and then it will not an easy thing for the hackers to misuse the data (Butcher, 2007).

4.12 Configuration Authentication

The phones of VoIP need to have the startup configuration for entering in to the system of VoIP and this configuration the VoIP phones can encounter with the issue of bootstrap problem in which it is very much hard for having the details of the unreliable invader. At the time of manufacturing, if it has been given the public key, which would be one of the good solutions of the configuring a secure server (Butcher, 2007).

4.13 Authenticating the signalling

There is connection between the phone of VoIP and the server which has been maintained by the SIP protocol and whenever the phone register with the server of SIP it shows its identity. This identity of the phone will be the physical address such as MAC address and logical address such as IP a protocol which is used mainly responsible for having the authentication and also for the encryption such as the IP security. This type of protocol is very much useful for having the maintenance of a tough authentication, which lies between the phone and the server, which is based on the haring keys with the phone, and the server. It is very easy for implementing on the small network but if there is large company then it becomes less effective such as in one case the key can be configured on the single system again it has some of the limitations. Alternatively, it would be introduction of the certification authority in the network and then last one is the setup of the DNS secure protocol (Butcher, 2007).

4.14 Encrypting the media

It is very important for securing the communication of VoIP from the access of unwanted invaders more specifically in the setup of an enterprise. There is a new version of RTP, which is known as the secure real time protocol SRTP, and it has been launched by the

Internet engineering task force as standard of RFC 3711. The main function of this is to authentication and then maintaining the confidentiality. It also works with the addition of the low overhead to the packet and then it lessons the numbers of key, which is used between two different points in the network. By decreasing the number of keys, which are shared between two points, still it needs a unique mater single key for the communication between two points (Pérez-Botero, 2011).

4.15 Vendors of VoIP Systems

Most of the companies in the market are now working for having more improved system of VoIP security. Among which Cisco and Nortel are most popular ones. They have started with the data network and they also have switched to the voice networks (Butcher, 2007).

4.15.1 VoIP systems by Cisco

The company has made the SAFE system for securing the communication of VoIP and the main function of this system is for securing the data network, servers and all other networks devices, which are used for connecting with the Internet and offices at remote locations and different enterprise (Butcher, 2007). The company has also developed the security in the communication of VoIP in very much efficient and secured way that has the following main factors in it: (Butcher, 2007).

- The company gives its support and also participate in the promotion in the usage of VoIP handsets as compared to the PC based IP phones.
- It also enables the use of dedicated firewall that will help in decreasing the DoS attackers.
- There is also an introduction of the separate address space for the Cisco IP telephony, which will be helpful in securing the session of VoIP.

4.15.2 VoIP Systems by Nortel

This company also has many security systems, which mainly have their focus on the requirements of enterprise for securing the IP telephony network. Nortel has defined its 4 different stages of security which are mentioned as follows:

- Minimum
- Basic

- Enhanced
- Advanced

Here there is the focus on the advanced level stage of security given by the company. This stage is further divided into 3 parts and it is considered that trust does not exist in any network (Butcher, 2007).

- The company used for implementing the MAC address security on all of the switches for checking an confirming the identity of the device and for having this implementation of the VLAN in switches for different types of data will come. Then these switches have to be intelligent enough to be able to monitor the attacks and misuse.
- In this company, there is the segment of voice which required to be retained for the IP phone and in case of the PC based, the phone firewall is must.
- The DoS attacks can be decreased by the use of DHCP, which is known as Dynamic Host Control Protocol server, which is able for managing the IP address in very effective way. Static IP can also be used for the next level authentication.
- There is also the use of dedicated firewall for the security of VoIP communication which is very good thing and foe making it sure that the voice zones are secure, the use of firewall will be helpful in decreasing the attacks by hackers.
- The encryption of the communication of VoIP by the use of IPSec channels is a kind of virtual private network that helps in maintenance of the security in communication.
- The company makes sure that there is a smooth running of the network and there is proper network set u end to end. The company has make it sure that there is occurrence of proper and error free communication and there is proper maintenance of all servers and on spot fixing of error is also implemented which is main key to success.

Chapter 5

Designing and Implementing Best Practices for Mitigating Threats Against VoIP

The implementations can be many, some protocols have been proposed to update the security measures and cut down the CIA threats. The acceptance of VoIP as a mainstream application has ensured that the research in this field keeps on moving in a fast-paced manner. The escalation is causing a high increase in need of a search for a proper security outline. This can be achieved by careful analysis and a lot of work to promote security measures and practices. Certain algorithms have been developed in this regard and more that can be developed and enhanced in future to sustain the VoIP networks.

The information security has many algorithms as well as security management systems including the ISOO series, out of which, the ISO17799 is the most widely adopted and has been used due to its focus on high security (Ramadan & Al-Qirim, 2015). There are a testing policy and parameters for removal of all possible vulnerabilities to maximize security. Also, the firewall settings, anti-virus packages and stepwise checkpoints for security vulnerabilities is one the most important feature of the system. The software security can be accessed by the possibility of remote access of all checkpoints. There is also the personal security option, which ensures that the confidentiality is maintained for all users and that the employees follow the necessary security protocols (Varma & Khan, 2015).

Networks that are publicly shared have a higher rate of security threats, which can be curbed by the implementation of security software packages and firewall. There are threats from sophisticated attackers who are equipped with enough knowledge to breach the security layers. These have to be tackled with great care and higher knowledge of security breaches and possible loopholes.

5.1 Most beneficial security algorithms

One of the most recent and strong security algorithms include the H.235, which is an authentic security framework designed to support data transfer and provides a stepwise, an end to end encryption that can minimize data loss due to the loss of compressed data packets. This security algorithm can be incorporated to support the basic H.235 systems. The security of data transfer and the signaling and media traffic control that has to occur during transfer or communications can be well controlled and monitored by using the H.235. The implementation of the framework has to be further analyzed to match the needs of the communication type and pattern under question or consideration. Also, this framework is yet to be modified and worked upon to make it run smoothly for the security of Internet-based data transfer (Phithakkitnukoon et al., 2008). Overcoming the barriers that hold back the existing algorithms with existing voice communication systems and security frameworks is hence extremely crucial.

The methods of security that are considered as relatively 'general' can be extremely beneficial when it comes to securing Internet-based connections and communications. Sometimes it is the very basic mistakes or overlooking of a minuscule detail that can lead to potentially big losses. Hence it is necessary to give careful consideration to even the very smallest of details when it comes to security.

5.2 Employee training for system security

One of the most important security measures is the proper training of all employees and personnel involved in software use, particularly those who are at any level involved in the IP based calls of the company. The users should be made aware of all threats associated with the use of IT systems and should be clarified about the points of the breach. The major reasons that can lead to accountabilities should be clear, and the policies of the company should be followed by one and all maximum ensuring security.

Before engaging people on an inner level or giving employees a clearance of the inner circle, certain measures of security should be kept in mind to make sure that the security access is not misused or breached. Those who are potentially not trustworthy should be kept away from the inner circle and security passes, and codes should not be shared widely.

5.3 Employee screening

Investigation of the employee's work and making a clear policy about penalties and consequences of security breaches is among the most crucial steps regarding security implementations. No matter what the position, all new employees should be thoroughly examined and screened for their level of trustworthiness. Similarly, the old employees should regularly be investigated about their work to make sure that there is no space left for cheating or possible security threats. Background checks should be very strongly implemented, and a team should be developed which keeps an eye on all security measures and also regulates the acts of all employees (Kandias et al., 2013). All sensitive information should be treated with great caution, and no documents or important passwords should ever be made public.

As it has been implied that insider threats are the biggest threats, these threats need to be identified, and all potential employees who might be selling important information to others should be identified and fired. Laws should be identified and stated which make them accountable and give them their due punishment according to the law. Identification is the very first step, but it has to be backed with strong evidence so that the person involved can be made to face the consequences that have been outlined by the law.

5.4 Detection of threats

The detection of threats is the most important implementation of security measures. This is better explained as screening measures. A definitive pattern of use should be determined for all users. Every individual should perform the same tasks as per the roles assigned to him or her. These patterns should be predetermined, and the training of a particular set of employees should be done according to the rules specified by them. Any deviation from pattern should immediately be identified and questioned as it can be threat to the security (Smith, 2015). The activity logs of all users should be carefully analyzed, and the baseline pattern of use should be regulated on a regular basis. The data not meant for users should be protected and kept away from them. Every employee should be assigned with only what concerns his or her duties.

5.5 Protection of information

The security implementations require a basic outline and policy that determines the right of information. Only the authorized personnel should have access to certain information.

Since the VoIP network is sensitive and requires very careful analysis of all possible threats, it is necessary to take security very seriously. Firms should protect their Internet access and also regulate all their IP based voice calls. Everyone who has access to these services should report their usage in company's log books and therefore be held accountable for their usage (Rhodes, 2013). This will develop a habit of careful reporting and impart a sense of responsibility and accountability.

Moreover, all-important documents present in the company systems should be password protected, and every access of these documents and data should be recorded, and each open and close of the session should require a security key. This will help ensure that no document is accessed or shared without the knowledge of the company peers. A complex system of passwords may although seem to be time taking but is essential in the long run (Machado et al., 2015).

5.6 Latest Session Initiation Protocol (SIP)

Some security measures can come in the context of latest security implementations. These include the H.235 framework as a strong and supportive security framework. Plus, the caller identification and detection of patterns to detect possible breaches are among the current championed methods. These have to be backed with strong algorithms and multi-layered frameworks that have security measures as essential tools. Continuous implementations and enhanced technology are making sure that the security threats and breaches are kept to a minimum.

Although all these countermeasures and threat minimizing initiatives are being implemented, they also help in making the VoIP a good experience for all users. However, there is no denying that the threats are running hand in hand with the increasing use of technology. This has to be kept in mind while opting for enhanced features and technology. Hence laws should be set which state the consequences of all breaches. The risk assessment and countermeasure of threats to the CIA concerns of VoIP should be backed with governance and suitable legislation. This along with all the latest technology and protocols help in making sure that the networks keep running fine and also keep serving the users with quality service.

5.7 Enhancement of user experience

Implementation of security measures can enhance the experience for all users and companies relying on VoIP. The major aim of this study was to identify threats and to put forward the best possible measures that can be incorporated to achieve the target of securing VoIP. Exploration of the threats regarding confidentiality, integrity, and availability of the VoIP networks. It has been seen that there is a low level of awareness about possible security breaches in VoIP. One of the easiest ways to upgrade the user experience is to make them aware of the different simple measures of security that they can themselves ensure. It is not always necessary to rely on experts for security. Certain security software can be downloaded on one's system, and the firewall can be updated to provide protection. Moreover, the easiest way is perhaps the setting up of passwords that can ensure the unauthorized users do not gain access to data not meant for them or that calls are not intercepted or eavesdropped upon.

Implementation of security checks and proper security measures are an absolute necessity to ensure that people do not lose their valuable data and information to unwanted strangers or potential enemies or business rivals. Plus, the security measures should be easy to understand to ensure that users do not find it more time to consume and problematic. Also, the overall load on the system should not be unnecessarily increased. There should be strong systems for compression and decompression of data packets when they are being transferred to minimize the bandwidth use and prevent choking of the network. Also, this helps in preventing packet loss.

5.8 Consideration of user expectations

The major goal of developing and implementing countermeasures of all threats is to enhance the overall experience of VoIP users. This can only be done by first understanding the expectations of the users and knowing what they see as threats? What is their level of understanding about the CIA threats and countermeasures? Our survey revealed that most people are using VoIP due to its low costs and high functionality. Whereas there is a question mark on the reliability of the networks that have been voiced by users. Many of the users working for large firms seem to have good knowledge about the way that VoIP works and the possible threats associated with it. Employees involved

in software and hardware usage of the Internet protocol-based voice calls are aware of the threats of integrity, availability and the confidentiality vulnerability.

Users have reported that there are constant security breaches and the encryption and security measures are compromised during voice packet transfer. It is believed that service providers should ideally also provide some security measures to protect the data of users. All these points and expectations have to be analyzed, and the security needs to be enhanced to meet the security standards and also the expectations of the users. Employees of firms relying on VoIP for their data sharing have emphasized the need to review the existing security measures and to go for an in-depth analysis of the existing protocols. It is extremely crucial to give due consideration to the expectations of users to receive a higher level of satisfaction and positive views in future. It is not only for the benefit of the users but also for the service providers as increasing the security measures will be good for increasing the reliability of VoIP.

5.9 Testing for best Practices

There is a need to focus on security implementations and make use of more than one security measures to be sure that the data is secure. Business firms need to minimize the access of important IDs and passwords, and only the most trusted and inner circle should have access to the security codes. Moreover, there have to be specialized algorithms for companies that are secure and can hold up the data and transfer using stepwise encryption and coding. A lot of measures need to be constantly searched and upgraded to continue combating all possible future threats, as these threats are likely to escalate with time and increase in the use of VoIP.

Chapter 6

Proposed VoIP Server Model

In this section, there is a comprehensive discussion about the c-based paralleled VoIP server model. The author was not able to implement the model due to lack of equipment so only the plan has been given. This model is what is suitable for the multi core and it can also base for the stimulation tool for the multi core SIP server and the main focus of this chapter is discussing the design of the client and server model. And the author has also made the design for a modular multi core server in C based. In the coming sections, there is also a description about the features of the model.

6.1 Introduction

The processors of the enhanced multi core are becoming the available every next some days in the industry of computing while the developers of software are not aware which the multi core can of for them. While writing the program of the computer, most of the developers give preference to extending or also enhancing the existing source codes which are by nature sequential. Parallelizes the existing source is not liked by the developers as it is very complex for doing and for giving no assurance of success and the transition from the sequential program to the parallel programs needs the analysis of the existing code of sequence and estimation of performance and verification which are achieved.

6.2 IOpenVoIP

A parallel client server model of VoIP is IOpenVoIP and it is used for the multi core server and the client as it is under the GNU which has its source code which is free for getting downloaded from the URL http://iopenvoip.lincisco.com and the main components of the system which are IOpnVoIP client and server as well. This also helps in communicating with the client to server for making the sessions of multimedia with

other clients in the Internet. It is also the concurrent server and it can also make many clients in same time. IOpenVoIP are intended for the audio, video and communication of data over the Internet. It is made in the GNU C.

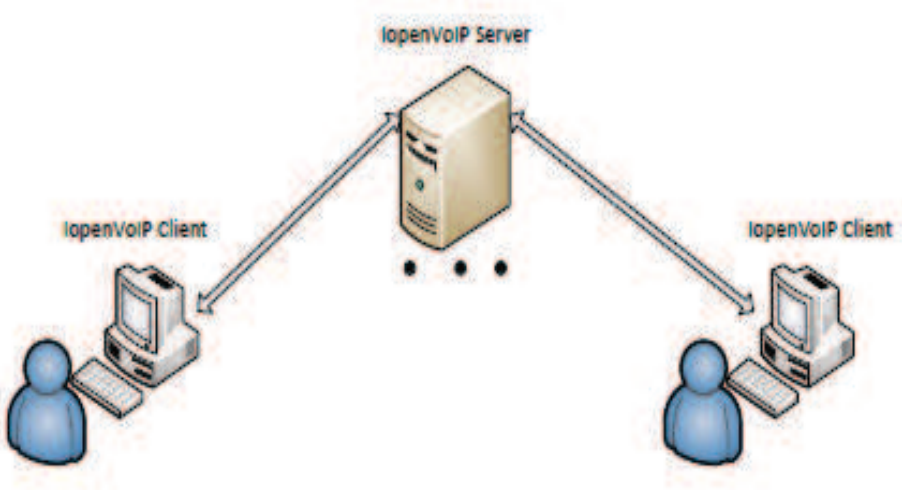

Figure 3: IOpenVoIP Server and Clients (Khan, 2011)

6.2.1 IOpenVoIP Server Features

All of the main components of the selected server are described as follows:

MYSQL Installation and Configuration

This is a relational management system of databases that is able to run as a server and it gives the multi user access to many databases. In this IOpenVoIP server also installs and also configures the MYSQL in automatic way with the Linux script for performing its operations.

Concurrent Server

This server is able for giving many clients requests in one time and it is also concurrent server.

Presence Server

It is known by this name as it is able for keeping the track of the user presence information and it is also able for sending the status information of the user. Easy configuration is

very easy for configuring and it can also be configuring by the text file with the code of the source.

Secure Communicatio

This component is able to encrypts all of the communication which is between the client and server and it also give supports all of the main encryption algorithms.

Flexible Source Code

It always keeps the future enhancements in mind.

6.2.2 IOpenVoIP Client Features

The main feature of the client is the followings.

User Registration

The registrations of the users can be done on the server with the client.

User Authentication

The supports of the client password-based authentication and the clients also take the user name and password and then they send it to the server for having the validations.

User Search

The search of the user makes the searching able other registered users on IOpenVoIP server.

Add Contacts

After having the successful search of the user there is addition of the contract function adds the contact information into the local database.

Contact status

This function is used for displaying the contracts presence information.

Audio and Text messages

From this function, the users are able for sending the audio and video messages to each other.

6.3 Server Design

The following figure is showing the modules of the server and also their interaction with each other. All of the numbers in the figure below shows step by step data flow of the server.

Step 1: When the program starts the module file reader loads configuration parameters, which starts from text file.

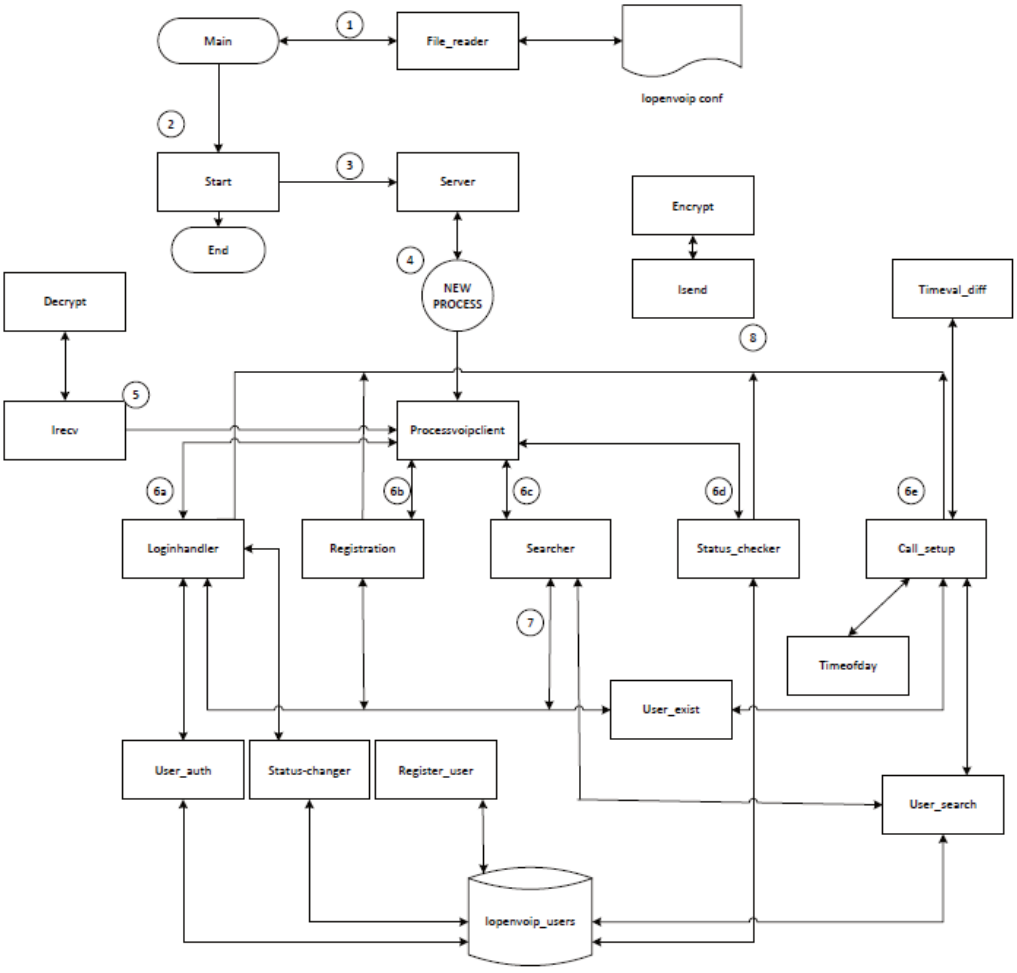

Figure 4: IOpenVoIP Server Design (Khan, 2011)

Step 2: The module of the start is like an interactive command line user interface which takes the configurations and commands from the administrator of the server.

Step 3: In the above-mentioned figure, the server module put the server into the listening state.

Ste 4: Whenever there is creation of the TCP and UDP connection to the server the UNIX fork functions makes the new child process for having the concurrency.
Step 5: In this step, there is reading of the irecv that the client buffers from the receiver and then they send it to the module for decryption.

Step 6: In this step the process VoIP cline module is like a parser which takes the request of the client from irecy module and then parse the string of the request and then it sends the parameters of it to the proper module for having further processing.

Step 7: In this step, the support is given to the IOpenVoIP user registration and authentication of the user, search of user, presence of them and also the setup of call. Other modules are driven by event and if the request is from the authentication of the user, then the handler of login and user make the modules perform the authentication. In this step, the module of the registration performs the registration if the request is for the registration of the user and if the request is regarding the presence of user then status checker module performs this function. On the other hand, if the request is regarding the call setup then call setup is used for this purpose for making the VoIP call.

Step 8: This is the last step in the process VoIP client module is used for sending the response to the send module that then encrypts it and then send it to the client.

The total duration of the call is estimated by time of day and time diff val modules. The server is used to then store the information of the user and all records of calls, passwords logins, and status if user in the local MYSQL database which is named as iopenvoip.users.

The above figure has been made by assuming that there is only one user who is connected to the server and only one process is running. The server has been made a new process for each client and then terminates the tear off connection.

Chapter 7

Conclusion

For making conclusions of the research it can be said that, VoIP has been utilized greatly on an individual and for different firms and organizations. From the level of general discussions to the level of making business-related phone calls, the utilization of VoIP has turned out to be very much incorporated into the daily use individuals and organizations around the world. Attributable to the immense utilize, the system faces a few dangers. The real threats against VoIP are identified with CIA concerns. The privacy of the information, as a rule, goes under inquiry when a lot of information exchange and vital dealings are completed over the VoIP. Likewise, an excessive number of clients prompt a rupture in the uprightness of the system, and the accessibility of administration additionally turns into an issue. A few examinations have done to investigate these dangers in detail and to keep up the security of VoIP.

The countermeasures have been investigated in accordance with the different sorts of concern. The security and insurance of information are guaranteed to utilize the most reasonable measures that can give methods for battling information robbery and break being used for credit by unapproved faculty. A standout amongst the most fundamental safety efforts that are utilized and can likewise help in ensuring that no undesirable individual gains admittance to one's information or captures calls through VoIP is the utilization of bona fide client ID and precisely set passwords or codes. These codes ought not to be shared and change frequently to keep the client IDs secured. Besides, the different interfaces that have been created to manage the systems and applications that give the administrations of voice bring over the web depend on different calculations all of which must be joined with some fundamental safety efforts. A general structure of

security has been investigated in this examination, and the different calculations for VoIP calls have been talked about alongside the fundamental security executions.

CIA threats have been investigated with incredible profundity, and the current breaks have been ascribed to different factors. The most widely recognized explanations behind breaks in security incorporate block attempt of calls by the unapproved workforce. The exploration questions decided for the investigation have been dissected inside and out, and it has been discovered that there is an excessive number of security dangers that must be routinely checked and handled. Some safety efforts have been investigated, and the inadequacies of every one of those strategies have been broken down also. The investigation has uncovered that there is plenty of hunts that still needs to go into the inquiry of safety efforts. Since the dangers are generally known, and the security ruptures are frequently experienced, the safety efforts must be extremely solid to battle those dangers. Mindfulness ought to be made a need above everything else, and each representative of the given organization ought to be prepared and educated to take after the security arrangements. The systems ought to be fused with appropriate safety efforts. Quite possibly security dangers can be recognized and identified so as to have countermeasures prepared so as to battle all dangers.

In short, the security measures have to be searched, implemented and constantly updated. There is a lot of research that still needs to be done to maximize security and minimize threats. Plus, there is a very good chance of newer algorithms for VoIP being proposed shortly due to the mounting use of Internet Protocol for voice calls, data transfer and also general conversations. Therefore, it becomes all the more necessary to develop strong security measures and create better ways that can be incorporated into the newer algorithms to ensure that the CIA threats are kept at the lowest possible rates. These security measures have to be reasonable, easily understandable and also incorporated with ease. These points if pondered upon and carefully planned, there can be a better experience for all users and the security of VoIP can be possibly enhanced to match its popularity and cost reduction.

References

Acharya, A., Kandlur, D.D., Mahadevan, P., Shae, Z.Y. and Singh, A. (2008). Enabling collaborative applications using Session Initiation Protocol (SIP) based Voice over Internet protocol networks (VoIP). U.S. Patent 7,376,129.

Aliwi, H.S.H. and Sumari, P. (2013). A comparative study of VoIP protocols. International Journal of Computer Science and Information Security, 11(4), 97.

Antwi-Boasiako, E., Kuada, E. and Boakye-Boateng, K. (2016). Role of codec selection on the performance of IPsec secured VoIP. In Advances in Computing, Communications and Informatics (ICACCI), International Conference, 2508-2514. Jaipur, India.

Assem, H., Malone, D., Dunne, J. and O'Sullivan, P. (2016). Monitoring VoIP call quality using improved, simplified E-model. In Computing, networking and communications (ICNC), 2013 international conference, 927-931, San Diego, CA, USA.

Azfar, A., Choo, K.K.R. and Liu, L. (2014.). A study of ten popular Android mobile VoIP applications: Are the communications encrypted? In System Sciences (HICSS), 2014 47th Hawaii International Conference, 4858-4867. Waikoloa, HI, USA.

Basem, B., Ghalwash, A.Z. and Sadek, R.A. (2015). Multilayer Secured SIP Based VoIP Architecture. International Journal of Computer Theory and Engineering, 7(6), 453.

Ben Chikha, R.J., Abbes, T. and Bouhoula, (2016). Risk Management for Spam over IP Telephony using Combined Countermeasures. In Proceedings of the 10th International Conference on Informatics and Systems, 240-246. Carthage, Tunisia.

Bilski, T. (2013.) New Threats and Innovative Protection Methods in Wireless Transmission Systems. Journal of Telecommunications and Information Technology, (3), 26.

Boehmer, W. (2013). How to Estimate a Technical VaR Using Conditional Probability, Attack Trees and a Crime Function. In International Conference on Availability, Reliability, and Security, 288-304. Springer Berlin Heidelberg.

Butcher, D., Li, X. and Guo, J. (2007). "Security challenge and defense in VoIP infrastructures", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37 (6), 1152-1162.

Callegari, C., Garropo, R.G., Giordano, S., Pagano, M. & Russo, F. (2009). A novel method for detecting attacks towards the SIP protocol. In: International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 268–273. Istanbul, Turkey.

Carvalho, L.S.G.D. and Mota, E.D.S. (2013). Survey on application-layer mechanisms for speech quality adaptation in VoIP. ACM Computing Surveys (CSUR), 45(3), 36.

Castellanos-Lopez, S.L., Cruz-Perez, F.A., Rivero-Angeles, M.E. and Hernandez-Valdez, G. (2013). Joint connection level and packet level analysis of cognitive radio networks with traffic. IEEE Journal on Selected Areas in Communications, 32(3), 601-614.

Dabbebi, O., Badonnel, R. and Festor, O. (2014). Leveraging countermeasures as a service for VoIP security in the cloud. International Journal of Network Management, 24(1), 70-84.

Dantu, R., Fahmy, S., Schulzrinne, H. and Cangussu, J, (2013). Issues and Challenges in Securing VoIP. Computers & Security, 28(8), 743-753.

De Rango, F., Fazio, P., Scarcello, F. and Conte, F. (2014). A new distributed application and network layer protocol for VoIP in mobile ad hoc networks. IEEE Transactions on Mobile Computing, 13(10), 2185-2198.

Deshmukh, R.V. and Devadkar, K.K. (2015). Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science, 49, 202-210.

Egan, B.P., Macaulay, R.P. and Vodesedalek, M. (2016). Rpx Clearinghouse Llc, Voice optimization in a network having voice over Internet protocol communication devices. U.S. Patent 9,264,325.

Eissa, M.M., Fayek, W.M., Hadhoud, M.M., Elmesalawy, M.M. and Shetaya, A.A. (2016). Frequency/voltage wide-area measurements over transmission control protocol/Internet protocol communication network for generator trip identification concerning missed data. IET Generation, Transmission & Distribution, 8(2), 290-300.

Fachkha, C., Bou Harb, E. and Debbabi, M. (2015). On the inference and prediction of DDoS campaigns. Wireless Communications and Mobile Computing, 15(6), 1066-1078.

Ghafarian, A., Draughorne, R., Hargraves, S., Grainger, S., High, S. and Jackson, C. (2007). Securing voice over Internet protocol. In Proceedings of the International Multiconference on ISSN, 1896, 7094.

Gruber, M., Hoffstadt, D., Aziz, A., Fankhauser, F., Schanes, C., Rathgeb, E. and Grechenig, T. (2015). Global VoIP security threats-large scale validation based on independent honeynets. In IFIP Networking Conference (IFIP Networking), 1-9.

Huang, Y. and Tang, S. (2016). Covert voice over Internet protocol communications based on spatial model. Science China Technological Sciences, 59(1), 117-127.

Huang, Y.F., Tang, S. and Zhang, Y. (2016). Detection of covert voice-over-Internet protocol communications using sliding window-based steganalysis. IET Communications, 5(7), 929-936.

Irshad, A., Sher, M., Rehman, E., Ch, S.A., Hassan, M.U. and Ghani, A. (2015). A single round-trip SIP authentication scheme for voice over Internet protocol using a smart card. Multimedia Tools and Applications, 74(11), 3967-3984.

Jayaprakash, M., Tamilarasi, A. & Gopikrishnan, S. (2012). QoS management in VoIP security using stream cipher', European Journal of Scientific Research, 87 (1), 127-136.

Jiang, Y., Tang, S., Zhang, L., Xiong, M. and Yip, Y.J. (2016). Covert Voice over Internet Protocol communications with Packet Loss Based on Fractal Interpolation. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 12(4), 54.

Keromytis, A.D. (2009). Voice over ip: Risks, threats and vulnerabilities. In Proceedings of the Cyber Infrastructure Protection (CIP) Conference, 223-240.

Lamba, R.K. and Kaur, K. 2014. Security traits of VoIP. Int J Res Advent Technol, 2(3), 178-181.

Lazzez, Amor (2014). VoIP Technology: Security Issues Analysis. IJITCS, 6 (7), 65-76.

Li, L.E., Mao, Z.M. and Rexford, J. (2012). Toward software-defined cellular networks. In 2012 European Workshop on Software Defined Networking, 7-12.

Liu, B., Zhao, B., Wei, Z., Wu, C., Su, J., Yu, W., Wang, F. and Sun, S. (2013). Qphone: a quantum security VoIP phone. In ACM SIGCOMM Computer Communication Review, 43(4),477-478.

Liu, G., Ji, H., Li, Y., Li, X. and Wang, Y. (2015). Transmission control protocol performance enhancement for the mobile broadband interactive satellite communication system: a cross layer approach. International Journal of Satellite Communications and Networking, 33(2), 119-133.

Liyanage, M., Braeken, A., Jurcut, A.D., Ylianttila, M. and Gurtov, A. (2015). Secure communication channel architecture for Software Defined Mobile Networks. Computer Networks, 114, 32-50.

Khan, Z. (2011). Design of VoIP Paralleled Client-Server Software for Multicore. (Msc Thesis). Royal Institute of Technology, Stockholm, Sweden.

Keromytis, A.D. (2009). Voice over IP: Risks, threats and vulnerabilities. In Proceedings of the Cyber Infrastructure Protection (CIP) Conference, 223-240.

Mazurczyk, W. (2013). VoIP steganography and its detection—a survey. ACM Computing Surveys (CSUR), 46(2), 20.

Mohammed, H.A., Ali, A.H. and Mohammed, H.J. (2013). The affects of different queuing algorithms within the router on QoS VoIP application using OPNET. International Journal of Computer Networks & Communications (IJCNC). 5(1), 117-124.

Negussie, S. (2013). Securing Confidentiality and Integrity of SIP Based VoIP System in Reduced Call Setup Time (PhD Thesis). Addis Ababa University. Addis Ababa, Ethiopia.

Niccolini., S. (2006). VoIP Security Threats. Draft of IETF Working Group Session Peering for Multimedia Interconnect (SPEERMINT).

Park, P. 2008. Voice over IP Security, Cisco Press. Indianapolis, USA

Pérez-Botero, D. & Donoso, Y. (2011). VoIP eavesdropping: A comprehensive evaluation of cryptographic countermeasures", IEEE Transactions on Networking and Distributed Computing (ICNDC), Second International Conference, 192-196.

Phithakkitnukoon, S., Dantu, R. and Baatarjav, E.A. (2008). VoIP Security—Attacks and Solutions. Information Security Journal: A Global Perspective, 17(3), 114-123.

Rathee, G., Bano, P. and Singh, S. (2015). A study various security attacks in wireless networks. International Journal of Computer Science and Mobile Computing, 4, 249-253.

Rathore, M., Paul, A., Ahmad, A., Imran, M. and Guizani, N. (2016). High-Speed Network Traffic Analysis: Detecting VoIP Calls in Secure Big Data Streaming. IEEE Transactions on Local Computer Networks (LCN), 41st Conference., 595-598.

Rhodes-Ousley, M. (2013). Information security the complete reference. Second Edition. McGraw Hill Professional. New York City, USA.

Rizvi, S.M.A. and Dowland, P.S. (2016). VoIP Security Threats and Vulnerabilities. Advances in Networks, Computing and Communications. 4, 114.

Satapathy, A. and Livingston, L.J. (2016). A Comprehensive Survey of Security Issues and Defense Framework for VoIP Cloud. Indian Journal of Science and Technology, 9(6), 1–13.

Shan, L. & Jiang, N. (2009). Research on security mechanisms of SIP-based VoIP system, Hybrid Intelligent Systems, HIS'09. Ninth International Conference on, IEEE. 408-410.

Schmitt, M.N., (2013). Cyber activities and the law of countermeasures. Peacetime Regime for State Activities in Cyberspace. 659.

Scholl, J., Lambrinos L., and Lindgren A. (2009). Rural telemedicine networks using store-and-forward Voice-over-IP. International Congress of the European Federation for Medical Informatics, 150, 448-452. Tromsø, Norway.

Shen, H., Cui, N., Wu, J. and Que, Y. (2016). NOKIA TECHNOLOGIES OY, Incoming call identification. U.S. Patent 20,160,134,750.

Singh, H.P., Singh, S., Singh, J. and Khan, S.A. (2014). VoIP: State of art for global connectivity—A critical review. Journal of Network and Computer Applications, 37, 365-379.

Smith, J.A., (2015). Mitigating malicious insider cyber threat. Technical Report RHUL-MA-2015-12, Information Security Group, Royal Holloway University of London, London, UK.

Stelkens-Kobsch, T.H., Hasselberg, A., Mühlhausen, T., Carstengerdes, N., Finke, M. and Neeteson, C. (2015). Towards a more secure ATC voice communications system. In Digital Avionics Systems Conference (DASC), IEEE/AIAA (34), 4C1-1. Prague, Czech Republic.

Wahab, A., Bahaweres, R.B., Alaydrus, M. and Sarno, R. (2013). Performance analysis of VoIP client with integrated encryption module. In Communications, Signal Processing, and their Applications (ICCSPA), 2013 1st International Conference. 1 - 6. Sharjah, United Arab Emirates.

Zhang, L., Tang, S. and Cai, Z. (2014). Efficient and flexible password authenticated key agreement for voice over Internet protocol session initiation protocol using smart card. International Journal of Communication Systems, 27(11), 2691-2702.

Zhang, L., Tang, S. and Zhu, S. (2016). A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP. Peer-to-Peer Networking and Applications, 9(1), 108-126.