iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** X **Month of publication:** October 2014

DOI:

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

Security on VoIP

Deepak Kumar[1], Deepika[2], Krishan Sharma[3]
Department of Computer Science, Dronacharya College of Engineering Gurgaon, India

Abstract*— Voice over Internet protocol (VoIP), is a way of communicating over Internet. It is one of the newest technology. There is an existing way of communication over any network. The Users can make the telephone calls over an IP network using this technology. This paper will describe Voice over Internet Protocol (VoIP) to a level that allows discussion of security issues and concerns. There are two kinds of spoofing attacks are possible, first one is IP spoofing attack and another is URI spoofing attack, which are described in this review paper. The Implementation of VoIP concerned by businesses, components of a VoIP system, and relevant security issues. The business concerns will be those which are used to affect the Quality of Service (QoS). The network components call processors, gateways and two of the more common architectures are held by VoIP.

***Keywords*— VoIP, H.323, SIP, MGCP, QoS, Spoofing Attacks**

I. INTRODUCTION

VoIP is a class of products that enable advanced communication services over data networks. While voice is a key aspect in such products, video and other capabilities (e.g., collaborative editing and whiteboard sharing, file sharing, calendaring) are supported. The key advantages of VoIP are flexibility and low cost. The former derives from the (generally) open architectures and software-based implementation, while the latter is due to new business models, equipment and network-link consolidation, and ubiquitous consumer-grade broadband connectivity.

Voice over Internet Protocol (VoIP) involves the transmission of telephone conversations using data connections that transmit packets of data based on an Internet Protocol (IP). The fundamentals of this technology have been around since the mid-1990s. Since then, VoIP (also known as IP telephony) has been one of the most important trends of the future for the telecommunications industry and for years has been the subject of numerous reports in industry and business media. While the heralded communications revolution initially took almost a decade to arrive, it has undoubtedly been picking up speed since around 2005.

To transmit voice conversations over a data network using IP, VoIP technology is used. Such data network may be the Internet or a corporate Intranet or managed networks which are specially used by long distance and local service traditional providers and ISPs (Internet Service Provider). Voice over Internet Protocol (VoIP) is a form of communication that allows end-user to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. A special type of adapter is used in some VoIP services which required a computer and a dedicated VoIP telephone. Other services allow to end-users to use own landline phone, it is used to replace VoIP calls. All these paradigms are held by a special adapter. Voice over IP refers to the diffusion of voice traffic over internet-based networks. Internet Protocol (IP) was originally designed for data networking for purpose of its success, VoIP protocol has been adapted to voice networking. The history of VoIP began with conversations by a few computer users over the Internet. Initially, VoIP required a headset to be plugged into the computer, and the participants could only speak with others who had a similar set up. They had to phone each other ahead or sent a text message, in order to alert the user at the other end of the incoming call and the exact time

We in this world are adapting the newest technology in order to make our life better and efficient. Over the last twenty years the cellular communication and landline communication have developed a lot and the cost are lowered a lot. Thus, VoIP technology emerges as a powerful competitors with the other cellular networks. It uses packet switching rather than the traditional circuit switching. It is the single network that supports various multimedia applications. In business, it is management's task to provide availability, cooperation of the resources or inputs in such a way that these goals are achieved efficiently for a successful industry the resources taken in consideration are financial, human, physical and information resources. The VoIP is used over the traditional telephony because:

- To lower the cost and to provide ease of access to customers globally.
- To make Technology more sophisticated.
- To use network available across globe effectively.

- Through the use of the Internet, customers have access to a wider range of information about products, markets and their competition.
- Customers have become more demanding in terms of price, features of technology, product's quality, delivery, quality of service, and responsiveness.
- To manage the expectation of customers.

The VoIP uses the packet switching network rather than the traditional circuit switching network. A VoIP telephone is connected to either a computer or a modem that is joined to the internet. It works same as cell phone , but your voice is digitized, divided into small chunks of data called data packets and compressed and then are sent over the net just as an e mail and are decompressed and hence are converted in to stream of voice signal at the other end i.e. at the receiver's end. These packets travel across the internet and reach their destination where they are assembled and are transformed into voice signals for the listener. This service can be delivered by a cable company or a VoIP carrier and testing is now being completed on providing internet over power lines.

II. IMPLEMENTATION OF VoIP

In this section first we will discuss VoIP protocols and after that data processing in VoIP, at last we will discuss about quality of service in VoIP systems.

A. Protocols

There are currently three types of protocols which are widely used in VoIP implementations: the H.323 family of protocols, the Session Initiation Protocol and the media Gateway Controller Protocol (MGCP). The discussion of these protocols is as follows:

1) H.323 Family of Protocols

H.323 [8], [9] is a set of recommendations from the International Telecommunication Union (ITU) and consists of family of protocols that are used for call set-up, call termination, registration, authentication and other functions. These protocols are transported over TCP or UDP protocols. The following figure.1 shows the various H.323 protocols with their transport mechanisms. H.323 family of protocol consists of H.225 which is used for registration, admission, and call signaling. H.245 is used to establish and control the media sessions. T.120 is used for conferencing applications in which a shared white-board application is used. The audio codec is defined by G.7xx series by H.323, while video codec is defined by H.26x series of specifications. H.323 uses RTP for media transport and RTCP is used for purpose of controlling RTP sessions. The following figure.2 & figure.3 shows the H.323 architecture and call set-up process.

2) Session Initiation Protocol (SIP)

The modification and termination sessions between two or more participants the IETF is used which is defined by SIP (session initiation protocol) [9]. These sessions are not limited to VoIP calls. The SIP protocol which is a text-based protocol, it is similar to HTTP and offers an alternative to the complex H.323 protocols. SIP protocol become more popular in comparison to H.323 family of protocol because it is more similar than it. The following figure.4 and figure.5 shows the SIP architecture, call set-up and tear down process.

3) Media Gateway Control Protocols (MGCP)

The communication between the separate components of a decomposed VoIP gateway is done by media gateway control protocol. It is a complementary protocol to SIP and H.323. "Call agent" is mandatory and manages calls and conferences, when we are using MGCP and MGC server (Figure 6). The MG endpoint is not responsible for calls and conferences. It does not maintain call states. MGs are responsible to execute commands sent by the MGC call agents. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under

B. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

C. Data Processing in VoIP Systems

There are three types of essential components in VoIP: CODEC (Coder/Decoder), packetized and playout buffer [10], [11]. The analog voice signals are converted into digital signals at sender's side, after that these digital signals are compressed and then encoded into a predetermined format using voice codec. There are various voice codecs developed and standardized by International Telecommunication Union-Telecommunication (ITU-T) such as G.711, G.729, and G.723 etc. The packetization process is performed by distributing fragmented encoded voice into equal size of packets.

Furthermore, in each packet, some protocol headers from different layers are attached to the encoded voice. Protocols headers added to voice packets are of Real-time Transport protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP) as well as Data Link Layer header. In addition, RTP and Real-Time Control Protocol (RTCP) were designed to support real-time applications at the application layer.

Although TCP transport protocol is commonly used in the internet, UDP protocol is preferred in VoIP and other delay-sensitive real-time applications. TCP protocol is suitable for less delay-sensitive data packets and not for delay-sensitive packet due to the acknowledgement (ACK) scheme that TCP applies. This scheme introduces delay as receiver has to notify the sender for each received packet by sending an acknowledgement. The UDP protocol cannot be applied to VoIP technology. It is more suitable for VoIP applications.

The packets are then sent out over IP network to its destination where the reverse process of decoding and de- packetizing of the received packets is carried out. The time variations of packet delivery (jitter) may occur in transmission process. Hence, a play out buffer is used at the receiver end to migrate the package without any interruption. Packets are queued at the playout buffer for a playout time before being played. However, these packets continued to arrive until the playout time is discarded. The fig.7 shows the end –to- end transmission of voice in VoIP system.

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

D. Quality of Service (QoS) in VoIP Systems

Quality of service (QoS) [3] can be defined as the network ability to provide good services that satisfy its customers. In other words, QoS is used for measurement of the degree of user satisfactions. When degree of user satisfactions is higher than it means the QoS is also higher. QoS are briefly described as given below:

1) Delay

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

2) Jitter

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

3) Packet Loss

Packets transmitted over IP network may be lost in the network or arrived corrupted or late. Packets would be discarded, when they arrive late at the jitter buffer of the receiver or when there is overflow in jitter buffer or router buffer. Therefore, packet loss is equal to the total loss occurs during congestion of network and late arrival. During the packet loss, the sender is informed to retransmit the lost packets. It causes more packet delay and it affects transmission QoS.

4) Echo

In VoIP, Echo occurs when a caller at the sender side hears the reflection of his own voice after he talked on the phone or the microphone, whereas the callee does not notice the echo. Echo is the term of the reflections of the sent voice signals by the far end. Echo could be electrical echo which exists in PSTN networks or echo of sound which is an issue in VoIP networks.

5) Throughput

The throughput may be defined as the maximum number of bits received out of the total number of bits sent during an interval of time.

III. CONFIGURATIONS OF VoIP

A. Dedicated routers

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

B. Adapters (USB)

USB devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters that are slightly larger than the typical thumb drive. They feature a standard modular phone jack to which you can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service.

C. Software-controlled VoIP applications: "softphones"

There are many software applications ("softphones") that allow you to place VoIP phone calls directly from an ordinary computer with a headset, microphone, and sound card. Internet telephony service providers usually give away their softphones but require that you use their service. Together, these applications and services enable users to talk to other people using the same service at no cost, and to the rest of the world for a fee. Software-based VoIP applications are quite attractive to consumers because they often already have most of the components necessary to get started at little to no cost.

D. Dedicated VoIP phones

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

IV. VoIP ATTACKS

A. Malformed Message Attack

Malformed Message Attack is one of the most representative cases using the vulnerabilities of text-based protocol. These attackers are able to cause malfunctions of proxy server by manipulating SIP headers. For instance, overflow-space, overflow-null, specific header deletion and using non-ASCII code are involved in these malformed message attacks.

B. SIP Flooding Attack

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

C. Spoofing Attack

Spoofing can be done when an attacker searches to be someone else in order gain access to restricted resources or steal information. This type of attack can take a variety of different forms; for instance, an attacker can change in the protocols which are used as the Internet Protocol (IP). The address of authorized user is given in order to get into their accounts. Also, an attacker may send fraudulent emails and set up fake websites in order to capture user's login names, passwords and account information. A phishing attack is any fake email or websites. Another type of spoofing involves setting up a fake wireless access point and tricking victims into connecting to them through the unauthorized connection.

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

D. Threats / Risks

Many of the threats associated with VoIP are similar to the threats inherent to any internet application. Internet users are already familiar with the difficulties of email abuse in the form of spam. VoIP opens yet another pathway for these annoyances, which can lead to spam over internet telephony (SPIT), spoofing and identity theft.

E. Spam over internet telephony (SPIT)

VoIP spam is unwanted, automatically dialed, pre- recorded phone calls using Voice over Internet Protocol (VoIP). It is similar to E-mail spam.

F. Spoofing

It is technically possible for an attacker to masquerade as another VoIP caller. For example, an attacker could possibly inject a bogus caller ID into an ordinary VoIP call so that the receiver believes the call to be coming from a known and trusted source. The receiver, fooled by the electronic identification of the caller, may place unwarranted trust in the person at the other end. In such an exchange, the receiver may be tricked into disclosing personal information like account numbers, social security numbers, or secondary authentication factor: a mother's maiden name, for example. This scheme is essentially the VoIP version of traditional phishing, where a user follows links in an unsolicited email and is tricked into providing personal information on a bogus web site. Attackers may use these bits and pieces of personal information to complete partial identity records of victims of identity theft.

G. Confidentiality concerns

The concern is that VoIP data sometimes travels unencrypted over the internet. Therefore, it is technically possible for someone to collect VoIP data and attempt to reconstruct a conversation. Although it is extremely difficult to achieve, some software programs are designed to piece together bits and pieces of VoIP data in an effort to reconstruct conversations. While such activity is currently rare, you should be aware of this possibility as it may increase as VoIP becomes more widespread.

V. How to Protect Against Risks

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

Enabling Voice VLANs raises the complexity to properly secure these physical Ethernet ports. Enabling without the proper security controls in place can increase the risk to an organization.

There are several types of the principles as well as the practices for safe VoIP usage are the same. However, you may already practice with other internet applications. There are some of the key practices of good personal computing:

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

VI. CONCLUSION

Security for a VoIP system should begin with solid security on the internal network. It should be protected from the threats of attached hostile networks and the threats of the internal network. The security policy should include any specific VoIP needs. The load of the VoIP system should be accommodated by the network and the servers involved, ensuring that proper resources are in place and available. A dedicated VoIP phone may consist of a phone and base station that connects to the internet or it may also operate on a local wireless network. Conducting a risk analysis of each component and process will identify the vulnerabilities and threats. This will provide the information needed to determine proper measures. There should be a proper valance balance between the security and the business needs of the organization. It is the key to the success of any

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

VoIP deployment.

REFERENCES

[1] H. Yong-feng, Z. Jiang-ling, "Implementation of ITU-T G. 729 speech codec in IP telephony gateway" Wuhan University Journal of Natural Sciences, Volume 5, Number 2, June 2000.

[2] M. Habib, N. Bulusu, "Improving QoS of VoIP over WLAN (IQ-VW)", Project Research Paper, for CS522 Computer Communications, University of Colorado at Colorado Springs, December 2002.

[3] P. M. Athina., A. T. Fouad and J. K. Mansour, "Assessing the Quality of Voice Communications Over Internet Backbones", IEEE/ACM Transactions on Networking, Vol. 11, No. 5, Oct. 2003.

[4] Qiu, P.Q., Monkewich, O., and Probert, R.L., "SIP Vulnerabilities Testing in Session Establishment and User Registration" ICETE (2), 223-229., 2004.

[5] J. B. Meisel, M. Needles, Voice over Internet protocol (VoIP) development and public policy implications, Info 7, 2005.

[6] Advisory Committee on International Communications and Information Policy (ACICIP), 2005.

[7] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice over IP Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-58, 2005.

[8] http://www.isoc.org/pubpolpillar/voip-paper.shtml 15.08.2006. http://www.eyeball.com/spit-solution.htm.

[9] K. M. McNeill, M. Liu and J. J. Rodriguez, "An Adaptive Jitter Buffer PlayOut Scheme to Improve VoIP Quality in Wireless Networks", IEEE Conf. on BAE Systems Network Enabled Solutions, Washington, 2006.

[10] C. Lin, X. Yang, S. Xuemin and W.M. Jon, "VoIP over WLAN: Voice capacity, admission control, QoS, and MAC", International Journal of communication Systems, Vol.19, No 4, pp. 491-508, May 2006.

[11] L. Mintandjian, P.A. Naylor, "A Study Of Echo In Voip Systems And Synchronous Convergence Of The µ-Law Pnlms Algorithm", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

[12] Seedorf, J., "SIP Security: Status Quo and Future Issues", Talk presented at 23rd Chaos Communication Congress, 2006.

[13] Russel, T., "Session Initiation Protocol (sip) Controlling Convergent Networks" McGrawHill Professional,2008