Collective Study On Security Threats In VOIP Networks

Muhammad Zulkifl Hasan, Muhammad Zunnurain Hussain

Abstract: The Collective study will critically evaluate the voice over internet protocol (VOIP) Security threats, issues & challenges in the communication over the network, the solution provided by different vendors. Authors will be discussing all security issues, different protocols but main focus will be on SIP protocol its implementation and vendors VOIP security system.

Keywords: (Voice over internet protocol VOIP), Session Initiation protocol (SIP), Real Time Transport Protocol(RTP), Media Gateway control protocol (MGCP), Internet Engineering Task Force (IETF), user datagram protocols (UDP), Multipoint Control Units(MCUs),

I. INTRODUCTION

Voice over internet protocol VOIP is a type of communication in which users can call each other using high speed internet rather using a phone. VOIP calls are very cheap and the industry is now shifting on this technology to save time, money and for reliable communication. The previous communication is using circuit switch network but now it has upgraded with IP-based packet switched networks. The basic structural components of the VOIP communication are the end points (telephones), control nodes, gateway nodes and IP based network. The IP network use different type of media like Ethernet, fiber and wireless for communication [2]. VOIP has improved the communication due to its more number of options likesharing of data , files, screen sharing and especially video chats. VOIP became more popular in the daily market use due to its cost and reliability. Number of companies are switching from old model of communication to VOIP calls i.e. Using Skype or video chat softwares for communication [3]. VOIP is a combination of multiple application protocols which are already running on the internet. As internet has no such specific design , so it makes the unwanted users to misuse the VOIP protocols. There are two main protocols used in VOIP .i.Signalling Protocol ,ii. Media Transport Protocol. Now a days Session Initiation protocol (SIP) and Real Time Transport Protocol(RTP) are the leading SIP & RTP protocols [4]. Now talking about the security issues , when VOIP applications will be used at offices the problem of security in terms of quality of service will arise. VOIP calls can easily be traced and tracked/ listened may be the attacker edit your communication or some confidentail conversation may be leaked or misuse while you are using the internet as it is an open system. The VOIP encryption techniques using some protocols will help to solve this critical issue [5].

- *Muhammad Zulkifl Hasan, Computer Science Dept NUST, NIPCONS engrrhasan@gmail.com*
- *Muhammad Zunnurain Hussain, Department of Computer Science, SCET Lahore engrrhusain@gmail.com*

II. SECURITY FEATURES OF FEW VOIP PROTOCOLS

For VOIP security and Qos , protocols which the writer will be discussing in this paper will be H.323,Media Gateway control protocol (MGCP),Session Initiation Protocol (SIP) .All VOIP protocols are application layer protocol and they work above to IP. i.e Internet Protocol .The VOIP protocols are mostly used on internet for the transportation of VOIP communication ,they are not limited to transmission control protocol TCP and user datagram protocols UDP. For SIP it is popular and mostly used for securing the communication. This protocol is a standardized by Internet Engineering Task Force(IETF). This protocol is designed for the two way communication sessions. It is not limited to VOIP calls. It has some features of HTTP text-based response structure. My main focus is on SIP as it is the leading protocol in VOIP and mostly used [3].

A. Protocol`s theory

1. H.323:

H.323 is the first multimedia communication protocol standard. ITU published it in Feb 1996. This protocol uses packet network for combining the voice, video and data. It has qualities of World Wide Web using PSTN at the back. The main components of H.323 architecture are Terminals, Multipoint Control Units(MCUs), Gateways, Gatekeepers, Peer and Border Elements. Every Component has its functionality like:

- Terminals are the termination points i.e. end points e.g Soft phones, Telephone etc.
- The MCUs are utilized for multi purpose conference calls.
- Gateway interface is used and referred to communicate between different protocols .
- Gatekeeper is not a compulsory component but it helps for call admission and address resolution. It can place direct calls to the end points or else where.
- Peer Elements swap the address information , and works inside the administrative domain [7].

This protocol specifies how the elements of the data i.e. voice,video can be transferred using the IP based networks [1].

i.Authenication: There are two types of authentication:

a. Symmetric encryption and
b. Asymmetric encryption

In symmetric encryption there is no specific requirement of pre-connection with any user. but in the asymmetric a preshared key needs to be shared before communication.

ii. Encryption: In VOIP the encryption will be packet based . It may vary with number of packets the policies and the rules [1].

2.MGCP(Media gatewaycontrol protocol):
This protocol is an IETF VoIP Protocol designed for residentail gateways, IP based phones and large trunks gateways [7]. This protocol is used for the communication between the different parts of VOIP gateways. It is corresponding protocol to SIP and H.323. This protocol is derived from set of other protocols i.e. SGCP & IPDC. The architecture of this protocol is , it contains a server called "call agent" which is controlling calls and other services. This gateway has to execute the instruction given by the server i.e. call agent [6]. Media gateway control protocol works on a call control architecture. It works like master slave protocol. This protocol divides the call control from the operational unit. It controls the media gateway [8].

3.SIP (Session Initiation Protocol):
SIP is different from H.323 as it is text based protocol . SIP is application layer protocol that means it will be carried by number of protocols i.e. Transmission control protocol and user datagram protocol with less overheads and its efficiency will be improved. It consists of a endpoints, a proxy server , location server and a registrar. Due to its location server it is popular and efficient [6]. SIP is widely used and easily available protocol . SIP works on two way communication pattern . It is like HTTP in some of the cases , like the authentication for users in HTTP. SIP is a signalling protocol which uses RTP for media transfer. The RTP protocol also has function to Secure & control the communication between the end users. SIP is using different transport protocols which are TCP,UDP & SCTP. All these protocols are used as they are easy to use and they have some good features over the other protocols .UDP is important as it maintains a level of performance, TCP is important as it helps in secure call setup,Stream control transmission protocol (SCTP) is important as it helps to reduce the DOS attacks [3].

B. VOIP Threats Details

- **Threats from humans:** These types of threats mostly focused on humans e.g. error in the configuration file, mismatch of protocols ,threats from unknown identity. Most Common Threats types will be phishing, theft of service , or unwanted contact [1].
- **VOIP Call alteration threats :** In this type of situation an unwanted user make a hidden link or connect himself in the conversation, changes call content and he himself ensure that nobody will capture him [9].
- **Denial of service threats:** refers to the term flooding in the communication traffic. In case of VOIP if somebody comes in between any conservation , this type of attack is very critical which ends up in losing some secret information and can be unmanageable by the comapny to face it [9].
- **Service abuse threats:** these threats refers to misuse of VOIP services i.e.non payment & billing frauds [1].
- **Physical Access Threats:** it is the unbearable threat in which someone comes in your envirnoment physically and destory the physical network .It is highest of lack of security [1].
- **Interruption of services threats:** These types of threats comes when something happens unexpectedly i.e. Act of GOD ,which blocks the VoIP Services e.g weather condition, natural disaster ,failure of services i.e. power etc which results in effecting the quality of services i.e. the quality of calls [10].

III. Overview of available Methods

These all threats can be overcome by implementing Session Initiation Protocol(SIP). As this protocol is the open source and these days mostly used in securing VoIP communication. Writer will be discussing SIP in detail i.e. its technical aspects, after implementation if any threat still come how to overcome that. SIP which is a application layer signalling protocol is very useful in the creation of sessions, modifying the previous ones securely, and finish the VoIP session/calls created between two users on the internet. SIP consists of different modules and servers i.e. "proxy, redirect, registrar, location servers and a user agent (UA)". The UA is basically the SIP phone which is connected at the termination point. The proxy server forwards the messages from the user agent to the given address. In the industry as cost is always an issue so most of the servers are logical and might be one server works for different jobs. All the specification described has been recommended by transport layer security (TLS) / IPSec to save and maintain the security level and requirements throughout the communication [4]. Now coming towards the SIP authentication it is same as the digest based HTTP authentication.SIP uses hash values for the authentication of message and maintaining its confidentiality. There are some security issues in the SIP authentication used these days which can cause serious problems like:

- The invader misuse /tap the conversation and use the important personal details like Bank Account or password/pins.
- The invader relocates /redirects the calls to somebody else without permission.
- The invader starts billing frauds with the caller without authentication.
- Interrupt and disconnect the current call [4].

IV. Possible solution after testing

In this section, Writer will be discussing some methods to secure the VoIP communication using some previous research.

A. Port Authentication

Port authentication is a very useful way to secure different communication. Port authentication uses the standard i.e. 802.1x to confirm the access between user and the authority. This type of authentication will help in securing the network. The invader has to first authenticate him with

the central authority then he will be given access which is very secure. But when the VoIP traffic joins the internet then this type of authentication fails and which lead to open access for invaders [2].

B. Categorisation of traffic

This categorization will help in securing the network as it has divided into different type of traffics like Voice and data. This will help in securing the network as the traffic divides so the probability of damage to the communication will be less and it will not be easy for the invader to misuse the data. As we have to two different networks i.e. one for voice other for data they will cost high. we need to implement the concept of Virtual Local Area Network (VLAN) in order to save money [2].

C. Configuration Authentication

The VoIP phones requires initial configuration to enter into the VoIP System. Configuring the VoIP phones encounter with the problem of bootstrap issue, in which it is difficult to have the details of an unreliable invader.At the time of manufacturing, if it has been given a public key that would be a solution of configuring a secure server [2].

D. Authenticating the signalling

The link between the VoIP Phone and the server has been maintained by the SIP protocol. Whenever a VoIP phone register with SIP server , it shows its identity. The identity of the phone will be its physical address i.e. MAC address and logical address i.e. IP A protocol is used which is responsible for the authentication & encryption i.e. IP security (IPSec). The protocol is very useful in maintaining a tough authentication between the phone and the server. The protocol is based on sharing of keys with the phone and the server. It is very easy for small network but in case of large organisation it has some different patterns i.e. In one case the key has to be configured on individual system again it has limitations. Second option would be the introduction of a Certificate authority(CA) in the network. and last would be setup a DNS secure protocol (DNSSec) [2].

E. Encrypting the media

It is very essential to secure the VoIP communication from the alteration or unwanted access especially in the enterprises setup. A new version of RTP called secure real-time protocol (SRTP) is launched by Internet Engineering Task Force (IETF) as RFC 3711 standard. The basic function of SRTP is to authenticate and maintain the confidentiality. It works like adding a low overhead to the packet and decreases the no. of key used between two different points in the network [2,11]. By reducing the number of keys shared between two points still it requires a unique master single key for the communication between two points.

V. VENDERS VOIP SYSTEMS

Many companies in the market is working on improving the VoIP systems security. Cisco and Nortel are those venders which started with data networks and switched to Voice networks [2].

A. VoIP systems by Cisco

Cisco developed a system SAFE to secure the VoIP communication. The basic functions of this system is to secure the data networks, servers, all those network devices connecting with internet, offices at remote location and different enterprise [2]. Cisco developed the security for VoIP communication in very effective and secured way. The Process has following key factors [2]:

1. Cisco support and promote the usage of VoIP handsets rather than PC-based IP phones.
2. The use of dedicated firewall will reduce the DoS attacks.
3. Introduction of separate address space for Cisco IP telephony will also help in securing VoIP session.
4. Port security and use of DHCP server will improve the VoIP communication and security will be improved.
5. User authentication is important point in maintaining a secure VoIP session. we have to configure a authentication system to minimize attacks.

B. VoIP Systems by Nortel

Nortel has many security systems mainly focusing on enterprise requirements to secure the IP telephony network. Nortel defines its four different stages of security i.e. minimum, basic, enhanced and advanced. Here we will focus on advanced level stage of security. It has further 3 levels/ stages of security. In advanced security level, it is considered that trust does not exist within the network [2].

1. Nortel implemented MAC address security on all switches to check and confirm the device identity. For this the implementation of VLAN in switches for different type of data will come. The switches have to be intelligent one to monitor the attacks and misuse.
2. In Nortel, the voice segment needs to be retained for the IP phone. In case of PC based phone firewall is must.
3. DoS attacks can be reduced using the Dynamic Host Control Protocol (DHCP) server which will manage the IP addresses very efficiently. Static IP can be used for next level authorization.
4. Use of dedicated firewall for securing VoIP communication is a good strategy. Making secure voice zones (SVZ) by the use of firewall will reduce the attacks by invaders.
5. Encrypting the VoIP communication using IPSec tunnels. Virtual Private Network (VPN) also helps in maintaining the security of communication.
6. Nortel make sure the smooth running of network and end to end connectivity in the network setup. Nortel make sure the appropriate and error free communication, proper maintenance of servers and on spot fixing of errors is key to success.

VI. CONCLUSION

In this collective study, authors have discussed the VoIP security issues, threats in detail. They described the protocols used to overcome this issue. As VoIP communication is very cheap way of communicating and these days very popular between the industry and for home users. They have also discussed two venders VoIP

systems which have switched from data networks to VoIP due to its demand in the industry. After discussing all the issues, threats in this collective study the authors have mainly focused on strengthening the protocols to reduce the attacks at different levels and also there should be some method to manage the security properly and new ways still required to improve the security [2].

ACKNOWLEDGEMENT

We would like to thank our mentors who guided us in finalizing this study. We would like to thank our Parents for their moral support and boosting our confidence in completing this in time .

REFERENCES

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

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

[3] Keromytis, A.D. (2011) 'A comprehensive survey of voice over IP security research', Communications Surveys & Tutorials, IEEE, 14 (2), pp.514-537.

[4] Zhang, R., Wang, X., Farley, R., Yang, X. & Jiang, X. (2009) "On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers", Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia New York, NY, USA: ACM. p61-69.

[5] Radman, P., Singh, J., Domingo, M., Arnedo, J. & Talevski, A. (2010) "VoIP: Making secure calls and maintaining high call quality", Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, Paris, France New York, NY, USA: ACM. p56-62.

[6] Kuhn, D.R., Walsh, T.J. & Fries, S. (2005) 'Security considerations for voice over IP systems', NIST Special Publication, pp.800-858.

[7] Soares, V., Neves, P. & Rodrigues, J. (2008) "Past, present and future of IP telephony", Communication Theory, Reliability, and Quality of Service, 2008. CTRQ'08. International Conference on, IEEE. p19-24.

[8] Lina, X., Xiuhua, T., Changyun, M. & Zhigang, W. (2010) "The design of enterprise VoIP MGC based on MGCP protocol", Networking and Digital Society (ICNDS), 2010 2nd International Conference on, IEEE. p526-529.

[9] Callegari, C., Garroppo, R.G., Giordano, S., Pagano, M. & Russo, F. (2009) "A novel method for detecting attacks towards the SIP protocol", Performance Evaluation of Computer & Telecommunication Systems, 2009. SPECTS 2009. International Symposium on, IEEE. p268-273.

[10] Shan, L. & Jiang, N. (2009) "Research on security mechanisms of SIP-based VoIP system", Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on, IEEE. p408-410.

[11] Pérez-Botero, D. & Donoso, Y. (2011) "VoIP eavesdropping: A comprehensive evaluation of cryptographic countermeasures", Networking and Distributed Computing (ICNDC), 2011 Second International Conference on, IEEE. p192-196.