ISSN 2278-7763

Performance Analysis and Security Provisions for VoIP Servers

Chirag Thaker, Nirali Soni, Pratik Patel

[1] Computer Engineering Department, L D College of Engineering, Ahmedabad, India. [2&3] Department of Computer Science, Rollwala Computer Centre, Ahmedabad, India.

[1] Email: chiragthaker@yahoo.com [2] Email: soni8010@gmail.com [3] Email: Pratik11886@gmail.com

ABSTRACT

The security issues are raising fast as many small and large scale organizations adopting VoIP communications. VoIP communication is a challenging aspect among security and preventive aspects for its service providers. Security tools are used to gain high level of performance of entire VoIP system. This paper provides the performance analysis of VoIP based servers providing services like IPPBX, IVR, Voice-Mail, MOH, Video-Call and also covers up the security provisions for securing VoIP servers.

Keywords: VoIP Servers, Security Hardening, Performance Analysis, VoIP Services

1. Introduction

VoIP allows the transmission of a voice and data over the network using internet protocol. As VoIP works over the internet, it becomes very popular target for the attacker. Many security tools for VoIP are available in the market today to achieve desired QoS. Many companies and organizations have already started adapting security programs such as vulnerability assessment tools, IDS/IPS systems and firewalls to address VoIP. In this analysis process we provide our VoIP server with IPPBX, MOH, IVR, Voice-Mail and Video Call facilities. All this features are provided by the Asterisk, which is open source PBX system. For the packet capture of the and the call analysis we use the Wire-Shark network packet capture tool. We also make the use of the tools like SIPp for the performance testing of the SIP protocol. This paper is organized as follow: section II present introduction to VoIP and its service, section III present requirement of VoIP services, Section IV present performance analysis of VoIP servers, section V describe security hardening and provision, section VI shows our conclusion.

2 .VoIP and its services

This section presents the overview of the VoIP system protocols and the services offered by the VoIP server.

2.1. Overview of VoIP protocols

In general, VoIP architectures are partitioned in two main components: signaling and media transfer [7].For the signaling Session Initiation Protocol (SIP) is use and media transfer is done with the H.323. SIP is a protocol standardized by the Internet Engineering Task Force (IETF).It is an application-layer control protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences [5].Fig.1 shows the SIP call flow. The end points are user Agent Client (UAC) or user Agent Server (UAS). The end points are, a proxy server, a registrar, a redirect server, and a location server. These entities initiate and receive sessions. They can be either hard-ware or software. The SIP UA send *INVITE* message to proxy servers and it is transferred to the another SIP UA.*OK* message is send when session established. Once an end-to-end channel has been established between the two endpoints, SIP negotiates the actual session parameters using the Session Description Protocol (SDP) to tear down session *BYE* message is send by any of the UAs.

ISSN 2278-7763

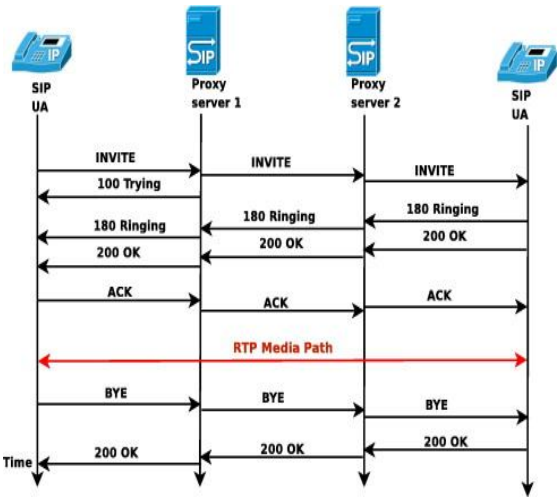

Fig 1.SIP Call Flow

H.323 is published by ITU and allows different communication devices to communicate with each other. Its protocol suit is designed to support for the multimedia communication and it is widely used in VoIP system [7]. Its main four components are end points (terminals), gateway, gate keeper and multimedia control unit (MCU) [13]. H.323 defines a general set of call setup and negotiating procedures.The most important in VoIP applications being H.225, H.235, H.245, and members of the Q.900 signaling series.The real-time protocols RTP and RTCP. H.323 also specifies a group of audio codecs for VoIP communications, the G.700 series [13].

2.2. VoIP Server services

Asterisk is the software that is installed to turn any computer into VoIP server [21]. Asterisk provides many services like call conference, voice-Mail, video-call, IVR (Interactive Voice Response), IPPBX, MOH (Music On Hold). The voice-mail feature provides capability for callers to leave messages when the called party is unavailable. Asterisk PBX supports a local voice-mail (VM) system that offers many options, including password protection, system greetings, e-mail notifications, and VM forwarding [2]. The music on hold feature provides music to a party waiting for its connection to be established. MOH can be triggered to play during call transfers, while waiting in queue for the next available representative or when the receiving party needs to mute the conversation. Conferencing allows for more than two parties to participate in a call and enables all parties involved to hear each other at the same time [1]. IVR automates routine customer service interactions by allowing callers to interact using touch tone digits or their voice. The basics to automate a routine, repetitive task is to reduce the require time and effort of an employee [1]. The IVR application is includes in automated attendance, password reset, voice surveys, account balance inquiries, flight status checks, rail-way inquires and package tracking.

3. Requirement of VoIP services

3.1 Basic requirement for VoIP

Before deciding to get VoIP service, we must consider the requirements that will be needed to make the most of VoIP. They are as follow**: 1)** ***A high speed broadband connection*** is an essential requirement for VoIP. You can use a DSL connection, a cable modem, a Wi-Fi network, etc. If you have a slow broadband connection, you will experience a lot of issues in sound quality with your calls and more of your calls may get dropped. 2)***An IP phone or analog phone with an adapter*** for VoIP communication you must have VoIP phone or if you using normal PSTN line then ATA enable you to plug in a standard analogue phone and use it to make VoIP calls. If you have decided to use your computer as your main VoIP mechanism, then you will need to purchase a Headset, Microphone and to install a soft phone in your system. The last requirement is a 3)***VoIP Service Provider (VSP***): Provider will supply you with an account and some form of Telephone Number.

3.2. QoS Requirements of VoIP

QoS (Quality of Service): It is a major issue in VOIP implementations. The issue is how to

ISSN 2278-7763

guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due interference from other lower priority traffic [15].***Voice (Bearer Traffic):*** QoS requirements and recommendations for voice 1) Voice traffic should be marked to DSCP EF per the QoS Baseline and RFC 3246, 2)Loss should be no more than 1 percent, 3)One-way latency should be no more than 150 ms, 4)Average one-way jitter should be targeted at less than 30 ms, 5)A range of 21 to 320 kbps of guaranteed priority bandwidth is required per call [20].***Packet Loss Ration:*** High PLRs have a severe impact on the subjective voice quality. CISCO recommends that the PLR should be 0 under nominal network load and link conditions to provide good quality. For acceptable quality under high network load and degraded link conditions the PLR should not exceed 1% [20]. ***Latency*****:** Latency can cause voice quality degradation if it is excessive.150 ms of one-way, end-to-end delay ensures user satisfaction for telephony applications. ***Jitter*****:** The variation of the delay has a major impact on the voice quality. Jitter buffers further add to the end-to-end delay, and are usually only effective on delay variations less than 100 ms [15]. Jitter must therefore be minimized.

4. Performance Analysis of VoIP Server & Services

VoIP network performance testing means the difference between a VoIP system working at a high level QoS and a weak system that runs so poorly. This section guides why it's necessary to have performance testing and some of the ways it can be done. We choose the VMware tools to have virtual environment for the implementation of the VoIP servers. We list out the following approaches on how to ensure the performance of the VoIP servers in the virtual network test bed.

1)*Analyzing the network to define best-case, average-case and worst-case scenarios*: These scenarios are set in test bed by providing the empirical inputs to the system. VoIP adopters record conditions on the production network over a long period of time and then play back those conditions in the lab to define scenarios [16]. By evaluating VoIP performance under these various scenarios, project teams can notice any problems that loom call quality. 2)*Use the virtual network to run VoIP services in the testing lab under those real-world scenarios* : After defining one of the above scenarios team can analyze VoIP testing by providing voice traffic between the every of the end points. 3)*Analyze call quality with QoS metrics*: After running VoIP traffic on the network, we examine the QoS parameters like delay, jitter and packet loss to determine the call quality. 4)*Validate call quality by listening to live calls*: Along with the QoS parameters we can also validate the call quality by generating and listing the call between any two end points in the test network. 5)*Repeat as necessary to validate quality remedies*: In the virtual environment we can have various scenarios and testing can be done without interrupting the production network. So the bugs are addressed and removed from the production network to achieve high degree of performance. 6)*Bring in end users for pre-deployment acceptance testing*: As the quality of voice is extremely subjective feature, many VoIP implement teams bring in end users for pre-deployment acceptance testing [16]. This lowers to be bothered about VoIP rebellion condition, where end users hesitate at call quality despite the best efforts of IT and the fact that call quality meets common industry standards.

7*)Continuously applying above best practices over time to have change in management process*: To maintain VoIP quality over time, IT organizations must combine the above best practices into their change management practices. It is for ensuring that change in location and new application on network will not affect end-to-end VoIP service levels [16].

Before implementing a VoIP network, it is important to look at all the factors to determine if

ISSN 2278-7763

the network will run as planned. We can also test the VoIP performance with the existing PBX system. For that we can configure the PBX system continues to function only dial plan entries are required to route calls between systems. By using the tools we can also test the VoIP performance. Different types of tools are available for the network scanning and packet generation and .In our experiment we use the SIPp for the performance testing. PacketScan, nmap, snmpwalk, fping, are packet, SIP-Scan, Nessus are various network scanning tools [17].

Security testing tools available are SiVuS and VoIPER. SiVuS is a SIP Vulnerability Scanner. VoIPER is a security toolkit that aims to allow developers and security researchers to easily, extensively and automatically test VoIP devices for security vulnerabilities.

A.*Testing of SIP protocol using SIPp*: SIPp is a performance testing tool for the SIP protocol. SIPp allows to generate one or many SIP calls to one remote system [11] .Syntax:/sipp -sn uac IP

./sipp -sn uac 192.168.100.124

B.*Traffic Control*: SIPp generates SIP traffic according to the scenario specified. You can control the number of calls that are started per second. By specifying parameters on the command line:

./sipp –sn uac –r 100 -rp 2000 192.168.100.124

This command run SIPp at 100 calls every 2 milliseconds.

- '-r ' specify the call "rate" in number of calls per seconds
- '-rp' specify the "rate period". This allows you to have n calls every m milliseconds.

5. Security hardening and provision for VoIP server

As VoIP systems increase in popularity so VoIP security issues are also increase**.** We list out the methods which are used to secure VoIP systems.

1) VoIP System Monitoring: Monitoring network traffic during peak usage times helps to identify any unauthorized users or network attacks [10]. **2) *Encryption***: All VoIP systems should use a form of Media (RTP channel) encryption to avoid the sniffing of VoIP data. All communications between network elements should be encrypted.**3) *Implement Network Intrusion Detection System***: It allows the host to discover a network security leaks before it is threatening [11].**4)*Use Strong Passwords*:** Strong password improves the security and hanging them often will discourage brute force attacks by hackers who use password cracking software to steal passwords and gain access to the network [4].**5)*Use Firewalls:*** Place IP phones behind a firewall and then implement safety controls to provide protection against networks attacks.**6)*Hardening the Base Operating System***: By stopping redundant services on the VoIP system improves security for the base operating system.**7)*Restrict SIP clients on IP addresses:*** Permit or deny access to a user based on their IP address, so that a particular user can connect and register only from the predefined IP address.**8)*Monitor critical files for changes*:** Monitor integrity of critical system files so that it is possible to detect intrusions into the system [2].

6.Conclusion

To protect your VoIP communications system use trusted Communication framework**.** The framework is built on open standards and architecture. Different approaches are there to ensure the performance of VoIP servers. By using various methods and tools described above we can protect VoIP system.

References

[1] Boris Pisarčík, ASTERISK Security Hardening Guide v1.0

[2] Florian Fankhauser, Maximilian Ronniger,' Security Test Environment for VoIP Research' In: International Journal for Information Security Research (IJISR), Volume 1, Issues 1/2, March/June 2011

[3] H.Schulzrinne and J.Rosenberg, \Internet telephony: Architecture and protocols an IETF perspective, "Computer Networks and ISDN Systems, vol. 31, pp. 237-255, Feb. 1999

[4] Hewlett–Packard:'Network-Hardning' 'http://www.techrepublic.com/whitepapers/network-hardening-access-control-switch-features/1725957

[5] J.Rosenberg, H.Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E.Schooler, \SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002

[6] Jim Van Meggelen, Jared Smith, Leif Madsen, Asterisk: The Future of Telephony, O'Reilly Media, September 2005. ISBN 978-0-596-00962-5

[7] Keromytis A. D., 'Voice-over-IP Security: Research and Practice', IEEE Security & Privacy, Vol. 8 No 2, 2010

[8] K.Shah , A.Thaker, 'A NOVEL APPROACH FOR SECURITY ISSUES IN VOIP NETWORKS IN VIRTUALIZATION WITH IVR' In: International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012

[9] M.Qadeer, A.Imrann 'Asterisk Voice Exchange: An Alternative to conventional EPBX' In: International conference on computer and Electrical Engineering, 2008.

[10] Mike Chapple, Enterprise Compliance: VoIP eavesdropping: Hardening network security to contain VoIP risks: http://searchsecurity.techtarget.com/tip/VoIP-eavesdropping-Hardening-network-security-to-contain-VoIP-risks

[11] PBXSecurity:http://www.telephonyyourway.com/2012/09/12/useful-tips-on-ip-pbx-security/

[12] Peter H. Gregory, VoIP Security For Dummies, Wiley Publishing, Inc. ISBN-13: 978-0-470-00987-1

[13] Thomas Porter 'Practical VoIP Security', Syngress Publishing, Inc., 2006. ISBN: 1597490601

[14] Testing your sip protocol via SIPp: http://freelinuxtutorials.com/quick-tips-and-tricks/testing-your-sip-protocol-via-sipp/

[15] Tim Szigeti, Christina Hattingh, 'End-to-End QoS Network Design':http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-in-9781587051760

[16] VoIP performance testing fundamental http://searchunifiedcommunications.techtarget.com/tutorial/VoIP-performance-testing-fundamentals

[17] VoIP Security Alliance, "VoIP Security and Privacy Threat-Taxonomy,version1.0." http://www.voipsa.org/Activities/taxonomy.php

[18] http://www.voipsupply.com

[19] http://www.thevoipstore.net

[20] http://www.voip-info.org/

[21] http://www.asterisk.org/