ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Performance and Security Challenge of VoIP

R. Sathish[#1], R. Sankar[*2]

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
rsathish156@gmail.com
[2]*Asst. Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
sankar@saec.ac.in

Abstract**—** Voice over internet protocol and transmission of voice over traditional packet switched IP network are one of the fast growing telecommunications. VoIP tenders lesser cost and suppleness; it can also bring in important jeopardizes and vulnerabilities. Security confronts of VoIP offers modification of voice, readdressing the call, protected voice and broadcast among two parties. Call holding times are collected through call detail records using SIP server, RADIUS server and PSTN gateways. The network components call processors, gateways and more common architecture are held by VOIP. Quality of Service (QoS) pass on to the capability of a network to offer improved service to precise network traffic in different technologies as well as Frame relay, Asynchronous Transfer Mode, Ethernet and 802.1 networks.

Keywords**—** Vulnerability; Significance; VoIP; Security.

1. Introduction

Voice over Internet Protocol (VoIP) technology let the users to create phone calls using a broadband internet link and for that we are using analog phone lines. VoIP holds great promise for lowering cost of telecommunications and increase of flexibility for both business and individuals [1]. VoIP is available in a wide range of services. Basic free VoIP services require all users to be at their computers to make or receive calls. Many small businesses are using VoIP and unique communications on their private networks. It is because private networks provide security and service quality than the public internet. The calling process convert analog voice signal to digital using analog-to-digital converter. Making a security to VoIP using eavesdropping, which monitor the victim's conversation and altering the voice, redirecting the call, accounting data manipulation, caller identification to make secure from the attackers. Session Initiation Protocol (SIP) is an application layer protocol can establish, modify / terminate the user sessions. Modeling the VoIP for call holding with two parties in between of SIP server, RADIUS server PSTN gateway.

2. Generic Security Concerns in VoIP

Implementation of VoIP is possible using VoIP protocols after data processing in VoIP, and quality of service in VoIP system. Others allow your call from a conventional handset or from a cell phone to any of the phone.

2.1 Dos

It is an effort by an assailant to put off the phone service from operating stipulations.

2.2 Eavesdropping

The conversation can be monitored by attacker. It includes data type conversations too. When A and B made a communication with each other and the assailant can observe the dialogues. Rational security is predictable in the phone structure and the communication that it carries.

2.3 Alteration Of Voice Stream

The attacker is able to listen to the conversation between two victims and also alter communications. The sender voice can be altered before the voice sent to the receiver. This could be easy to change very small portions of a conversation.

2.4 Call Redirection

The single phone number has the ability to readdress to the proprietor is whenever needed. A superior characteristic gives the caller a simple way to discover a person by dialing a solitary phone number. This rich characteristic will be a latent risk, if the redirection characteristic becomes negotiated by an attacker.

2.5 Accounting Data Manipulation

These call data records contain data about the numbers the call was placed from, time of call, duration, and other information. By gaining access to the CDR database, the attacker can view call patterns.[2].

2.6 SIP Registration Hijacking

SIP is an app layer etiquette that can institute, modify and terminate user sessions. Registration hijacking can result in loss of calls of targeted user agent. SIP message modification: The person being called in session initiation message, changing some or all of attributes of the message. By modifying, the attacker could reroute a call to an unintended party. Currently, UDP and TCP are used to carry registration information between the user agent and the control node.

2.7 SIP cancel/bye attack

The attacker can create SIP message with Cancel or Bye command in its payload and send it to an end node to terminate an ongoing conversation. By adding strong authentication to the communication between the UA and the control node, this type of attack can be prevented[5].

3. Message Flow for Call Setup

Step 1: The calling party sends an INVITE message to the SIP server. This message includes a Request header field to the called party, a From header field indicates the calling party, a To header field indicates the mobile called party, and several authentication parameters.

Step 2: In the reception of the INVITE communication, the SIP server performs as a RADIUS client and propels an Access-Request communication to the RADIUS server. The Access-Request messages have the authentication parameters.

Step 3: The RADIUS server retrieves the user's record from its database by using the authentication parameters. Then it replies with an Access-Accept message to the SIP server to authorize the SIP request. At this point, the username parameter is confirmed.

Step 4. After Access-Accept from the Radius server to SIP Server, The SIP Server sends the INVITE message to PSTN Gateway.

Steps 5–8: The PSTN gateways put up an Initial Address Message (IAM) and propel it to the mobile network of the caller. After the called party pick the call and the mobile network reply with an Answer Message (ANM) to the PSTN gateway. The PSTN gateway build a final response message 200 OK. This message is route the calling party And this message is sent to the SIP server then moved to the calling party. The calling party replies an acknowledgement message to the PSTN gateway to conform the acknowledgement of the 200 OK message. The acknowledgement message is sent to the PSTN gateway by the SIP server.

Steps 9–10: The SIP server propel an Accounting-Request message with a status as "start" to the RADIUS server to generate a fresh call data record for the assigned mobile VoIP call. This message includes the username (8930001). In the formed record, the username is established at step 3, the SIP address constraint is the IP address of the SIP server, the estimated start time constraint is regained from the local timer, and the calling station ID constraint is recovered from the title field of the Accounting-Request message. The called station ID parameter is retrieved from the To header field of the message sends receipt of the request message by using an Accounting-Response message containing the radiated accounting id parameter (10243) to identify the call data record.

Steps 11–12: The called party hang on the call when the conversation is complete. The mobile network sends the PSTN gateway a release message to terminate the call. The PSTN gateway then produces a BYE message and propels it to the caller from side to side the SIP server.

Steps 13–14: After the caller ends the call, it sends a 200 OK acknowledgment communication to the PSTN gateway by the SIP server. The 200 OK communications decides that the call is fruitfully finished at the caller. The PSTN gateway produces a Release Complete (RLC) communication to the caller and discharged the communication aloof for this call.

Steps 15–16: The receipt of the 200 OK message, the SIP server sends an Accounting-Request message with notification "stop" to the RADIUS server. This message includes the radiated accounting id parameter (10243) received at step 10, the accounting stop time parameter (2006-06-22 09:02:44) retrieved from the local timer, and the accounting terminate cause parameter (User Request) that indicates the call is terminated by the user. The RADIUS server calculates the accounting session time parameter (00:01:12) and fills the parameters into the call data record. Finally, the RADIUS server sends an Accounting-Response message to the SIP server[3].

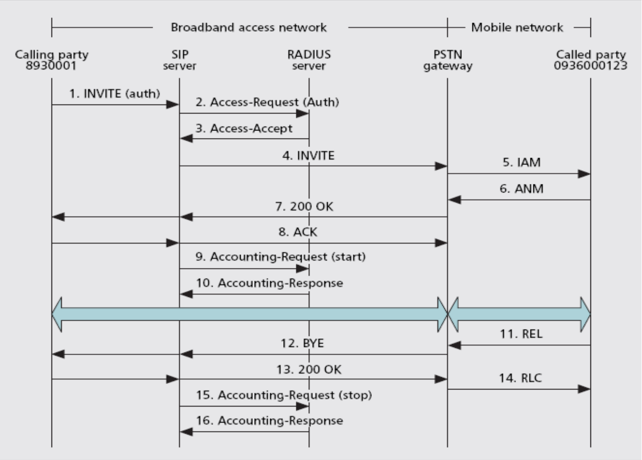

Fig. 1: Call setup and call release message flow mobile network and broadband

3.1 Quality of Service(QoS)

Quality of service means the network ability to provide good services that satisfy its customers. VoIP has brought in the necessities for data packets to arrive at the destination in an exact controlled time than other internet protocol functions. Several applications are rather tolerant of packets interruption and it may be unnoticeable to the user. Packet holdup in VoIP can decrease the activity to unusable. This delay management is known as QoS.

A. Delay

Delay defined as the total time it takes a person communicating to another person and hearing them at the other end. Delay can be of three types: Delay at source, delay at the receiver, and network delay.

B. Jitter

IP network does not guarantee of packets delivery time which introduces variation in transmission delay. Jitter can cause long delays before packets arrive and can cause packets to get out of sequence.

C. Packet loss

Packets transmit over internet protocol may be lost or arrived late. Packets will be surpluses, when they turn up delayed at the jitter buffer to the recipient or run over in jitter buffer or in router buffer.

D. Echo

Echo occurs when a sender side caller hears the reflection of his own voice after he talked on phone. Echo could be electrical echo which already exist in PSTN networks or echo of sound which is an issue in VoIP.

E. Throughput

The maximum number of bits received out of total number of bits sent during an interval of time[4].

4. Conclusion

This paper bring to a close the unique safety concern to VoIP systems as well as issues ordinary to conventional IP data networks and evaluates a few issues with security in PSTN networks. A dedicated VoIP phone may consist of a phone and base station that connects to the internet or it also operate on a local wireless network.

5. Future work

The extension of the link layer error may control the scheme with Forward Error Correction. Future evaluations of speech quality should have advantage of advanced results in the speech quality measurement domain.

References

[1] P. Mehta and S. Udani, “Overview of voice over IP”, Dept. Comput.Inf. Sci., Univ. Pennsylvania, Philadelphia, PA, Rep. MS-CIS-, vol.3,Feb.2001, pp. 01-31

[2] David Butcher, Xiangyang Li and Jinhua Guo, “Security Challenge and Defense in VoIP Infrastructures”, IEEE, Vol.12, 2012, pp.45-67.

[3] Whai-En Chen, Hui-Nein Hung and Yi-Bing Lin, “Modelling VoIP call holding Times for Telecommunications”, National chiao Tung University, 2008, pp.82-85.

[4] Greg S. Tucker, “Voice Internet Protocol VoIP Security” GIAC Security Essentials Certification, Practical Assignment, version 1.4c, option, Vol.3 October 2004, pp.35.

[5] Russel, T., “Session Initiation Protocol (sip) Controlling Convergent Networks” McGrawHill Professional, 2008, pp.46.