Performance Analysis of Various Encryption Algorithms for Locating Sip Users in Voice Communication

Dr.N.Arumugam
Lecturer (SG), Dept of ECE, Nachimuthu Polytechnic College, Pollachi, Tamilnadu, South India

Abstract **- Voice over Internet Protocol (VOIP) is a fast-growing technology believed to be the future replacement for traditional Public Switched Telephone Network (PSTN) networks. VOIP offers many benefits over PSTN, but when it comes to service it has many issues on reliability and security. One of the major issues is to identifying the communicating parties on the Internet in a secure and reliable manner. The Session Initiation Protocol (SIP) is used to creating, modifying, and terminating sessions between the participants. But the existing security mechanisms in the Session Initiation Protocol are inadequate for cryptographically assuring the identity of the end users that originate SIP requests. This paper is analysis the performance of different encryption algorithms for locating SIP users in voice communication.**

Index Terms **- SIP, Security model, User Agent Server, User Agent Client, Authentication, Repository, Encryption, Decryption**

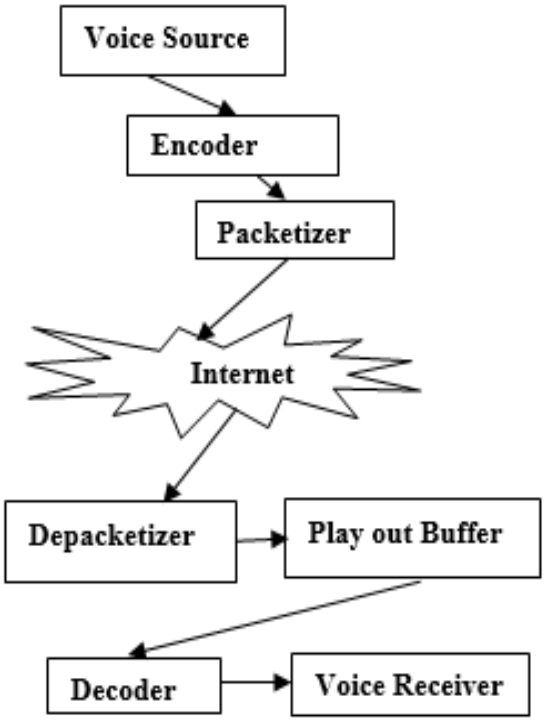
I.INTRODUCTION

A. VOIP System

Voice over IP (VoIP) – It is an IP based voice communication system using the internet protocol (IP) to transfer voice communications between two parties. The voice signals are digitized and packet zed.

The packets are sent across the Internet to a destination server where the packets are re-assembled. Thus, in real-time two or more people can make conversation with minimum requirements [5]. The fig 1 shows the various components of Voice Communications over Internet system [6]. Due to technical, commercial, and legislative reasons, measuring the sound quality in VOIP environment is a basic requirement of modern multimedia communication systems [15]

Fig 1: Various Components of Voice Communications over Internet system



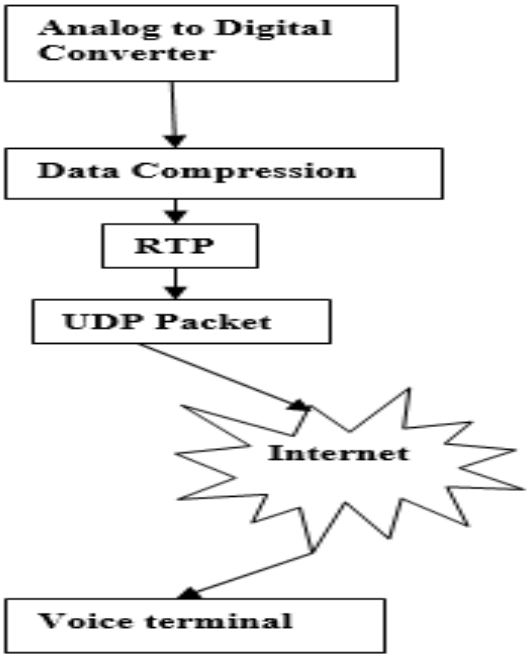
B. VOIP- basic process

The basic process which is involved in a VoIP call is as shown in the fig 2.

The processes are as follows:

1. Conversion of the caller's analogue voice signal into a digital format.
2. Compression and translation of the digital signal into discrete Internet Protocol
3. packets.
4. Transmission of the packets over the Internet or other IP-based network.
5. Reverse translation of packets into an analog voice signal for the call recipient.

User A



User B

Fig 2. VOIP- basic process

C. Encoding schemes

Encoding is the process of transforming information from one format into another format.

There are many encoding schemes have been developed and standardized by the International Telecommunication Union (ITU). This project is preferred G.711 since it is simple and using sample-based Pulse Code Modulation (PCM) which will produces a digitized signal of 64 kb/s [6].

D. VoIP Protocols

To transfer voice communications between two parties on internet different protocols are used. In data network different layers are exist for transferring data. Table 1 shows different types of VoIP protocols and its layers along with its equivalent's protocols.

Table 1: Different types of VoIP protocols and its layers along with its equivalent's protocols.

VoIP protocols	layers	Internet Equivalent	OSI MODEL
SIP	7	HTTP	Application
H.323	6		Presentation
RTP, RTCP	5	SSL	Session
UDP	4	TCP	Transport
IP	3	IP	Network
DATA	2	Ethernet	Data
Physical	1	100-Base T	Physical

E. Requirement to make a VoIP call

To make a VoIP call, the user requires VoIP software and a broadband internet connection. The software can be installed on a variety of hardware devices like telephone handsets, PC, Personal Digital Assistant (PDA) etc. This type of software-enhanced end-user devices is one of the key distinguishing features of VoIP. In addition to the above VoIP service provider is also required. Different types of VoIP service are available some of them provides support only for PC-to-PC calls, while others provide support to make and receive calls using IP enabled devices [7]. The quality performance of VoIP services was analyzed [8]

II. THE SESSION INITIATION PROTOCOL (SIP)

A. Introduction

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol used to creating, modifying, and terminating sessions with one or more participants. These sessions may be an internet telephone call, or a multimedia conference. SIP does not provide any services, but it is used to implement different services. SIP works with both IPv4 and IPv6.

B. Need for SIP

Voice communication over IP is a peer-to-peer connection i.e., a terminal device should be able to contact another terminal based on IP address on the internet. The called party location is identified on the internet before a media session is established. For large scale public use some infrastructure support is needed in order to locate the communication endpoints [7]. As per the RFC 3261 the SIP protocol is used for this purpose.

C.SIP Functionality

Since it is an application-layer control protocol used to establish, modify, and terminate multimedia sessions like internet telephony calls. The five facets of establishing and terminating multimedia communications are:

User location: determination of the end system to be used for communication.

User availability: determination of the willingness of the called party to engage in communications.

User capabilities: determination of the media and media parameters to be used.

Session setup: establishment of session parameters at both called and calling party.
Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

D. SIP Components and Message

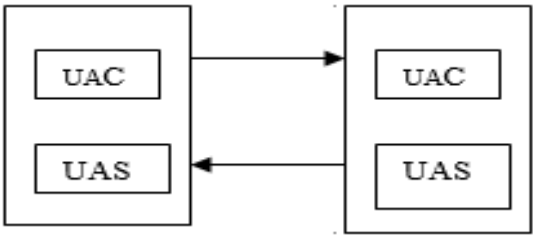


Fig 3 SIP Agent communication

The user agent client UAC and user agent server UAS are two key components in the SIP base network. The fig 3 shows the communication between the UAC and UAS.

User Agent Clients (UAC)
In VoIP, UAC is an entity used to initiates a call i.e. a client application in an SIP system that initiates the SIP request used to send to the UAS.

User Agent Server (UAS)
In VoIP, UAS is an entity used to receive i.e. a server application in an SIP system that accepts the requests from a UAC and generates an accept, reject, or redirect response on behalf of the user.

SIP user agent:
The combination of the UAC and the UAS is called the SIP user agent. The SIP user agent allows peer-to-peer calls to be made using a client-server protocol. Both UAC and UAS can terminate a call.
In general UAC initiates the SIP request while the UAS contacts the user when a request is received and returns a response on behalf of that user. The response may be an acceptance, a rejection, or a redirection of the request [8].

E. SIP Architecture
In the SIP architecture different types of server are used to perform specific functions within the network as in the fig 4.
A proxy server makes requests on behalf of other clients.
A redirect server accepts a SIP request maps the address into another address and then returns the new address to the client.
The registrar server accepts REGISTER requests and may be co-located with the proxy or redirect servers.

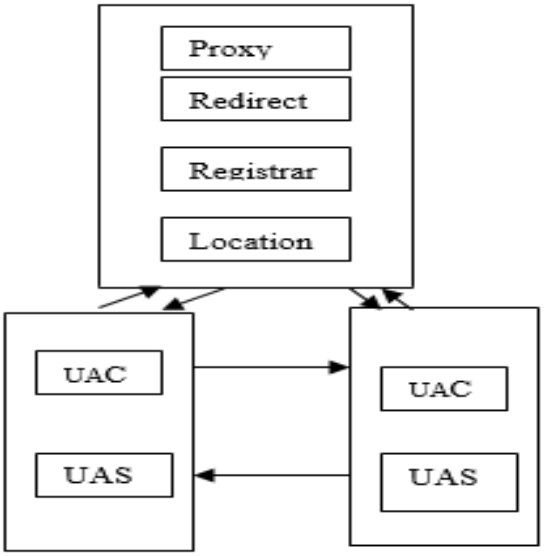
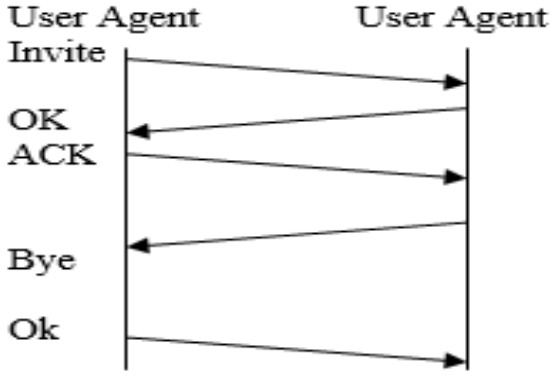


Fig4. SIP Agent and Server Communication.

Finally, the location server provides a service to the proxy or redirect servers by obtaining information regarding the callee's possible location. Location server may also be co-located with another sip server.

F. SIP Signaling
SIP is not as complex as H.323.The session between two user agents is illustrated in the fig 5. The process begins with the caller user agent sending an INVITE message to the called user agent including the calling party address and the description of the session [8].



G. SIP Messages – Methods and Responses
SIP Methods:
INVITE – Initiates a call by inviting user to participate in session.

ACK - Confirms that the client has received a final response to an INVITE request.
BYE - Indicates termination of the call.
CANCEL - Cancels a pending request.
REGISTER – Registers the user agent.
OPTIONS – Used to query the capabilities of a server.
INFO – Used to carry out-of-bound information, such as DTMF digits.

SIP Responses:
1xx - Informational Messages.
2xx - Successful Responses.
3xx - Redirection Responses.
4xx - Request Failure Responses.
5xx - Server Failure Responses.
6xx - Global Failures Responses.

H. Process for Establishing Communication

The following steps are used to establishing communication between two parties on internet.

1. Registering, initiating and locating the user.
2. Determine the media to use – involves delivering a description of the session that the user is invited to.
3. Determine the willingness of the called party to communicate – the called party must send a response message to indicate willingness to communicate – accept or reject.
4. Call setup.
5. Call modification or handling – example, call transfer (optional).
6. Call termination.

III. EXISTING SYSTEM

In the existing system during the client registration each client has to generate and registers its key pair in its local registrar. The registration may go through some out-of-band channel or out-of-band verification. And also, the issue of authentication is not explicitly addressed. For the integrity protection in the existing system passes a self-signed user certificates or plain user public key which may leads to man-in-the-middle attack since user public key is not authenticated. In certain situations, there are ways to detect such attacks [9], but not to prevent them.

IV. PROPOSED SYSTEM

To identify the SIP user in a secure manner each client has to sends a REGISTER message to the Registration Server. During the initialization between two parties, the caller sends an invite message along with header information about its identity. Caller receives its identity when it is verified by the server. The same procedure will be implemented for the called party also. Thus, the intruder's involvement will be eliminated. After completion of initialization process, the information messages are encrypted using the SHA algorithm to provide authentication. The bilateral communication will be established between the callers after performing the decryption process to avoid the man in middle attack.

A. Registration SIP

A Registration SIP procedure is shown in Fig 6.

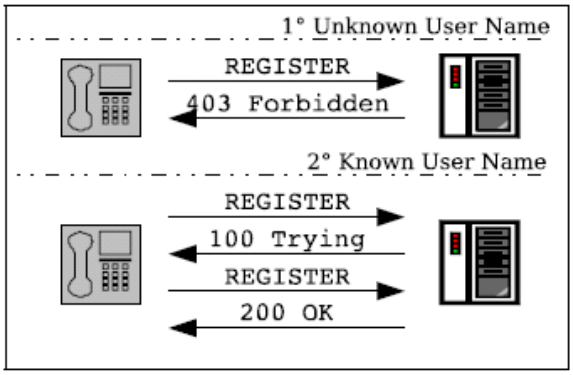


Fig.6. SIP Registration Flow

1. The user sends a REGISTER message to the Registration Server.
2. If the username exists as a valid user on the server list, a reply with a 100 Trying message containing a challenge to authenticate the user is received and we continue in the next step. Otherwise, if it does not belong to this list a 403 Forbidden message is send and the registration session is over.
3. If the server sends a 200 OK message the user was accepted.

B. Initialization SIP call

A simple initialization SIP call between two parties flow is shown in Figure 4 and proceeds as follow.

Fig. 7 SIP Call Flow

1. The caller party sends an INVITE message to the other party.
2. The called party acknowledges the INVITE message and replies with a 100 trying message.
3. As soon as the called party is ready to ring, it sends back a second message 180 Ringing.
4. When the called party answers the phone, it sends 200 OK messages. Now both parties start to send packets.

C. SIP Security model

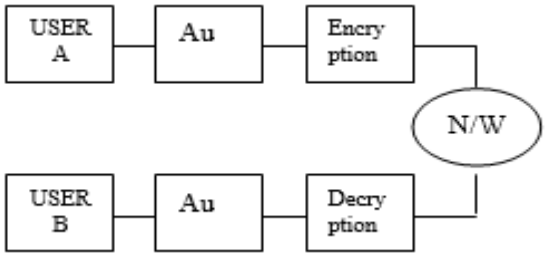


Fig 8: SIP security model

The Identity-Info header contains an Identity from which its certificate can be acquired. Connection is established between User A and B. Signature of both user A and B are verified.

Identity-Info header

In order to have a bilateral communication between the parties the identity information header is verified which contains the identity of user [4].

Signature verification

The Digital Signature Algorithm (DSA) is used for signature verification. DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process.

Message Authentication

Message Authentication is generated using SHA algorithm which depends on both the message and some (public or private) key known only to the sender and receiver. The message may be of any length but more often is some fixed size. The SHA hash function condenses the message to the required size. After adding the header info, the data packet is encrypted by means of the Secure Hash Algorithm [10].

V. EVALUATION

Experiments are done for different user load which are encrypted using DES and RSA algorithms. The voice signals are recorded and stored in encrypted format during the capture period. Encrypted voice signals are decrypted during the play back time. Depends on the vowels which are used for the evaluation the encrypted file size is also varied. The encrypted file size will also vary depends on the modulation of the voice signals. High frequency voice signals have larger encrypted file size similarly lower frequency voice signals have lower encrypted file size. Fig 9 shows the comparison chart for different load size Vs response time for RSA algorithm.

The fig 10 shows the comparison chart for different load size Vs response time for DES algorithm.

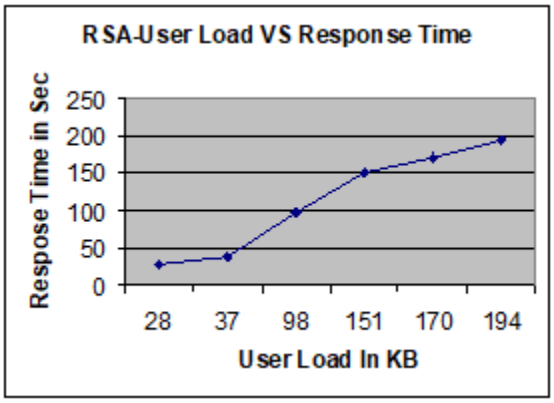


Fig 9 Comparison between user load with response Time for RSA

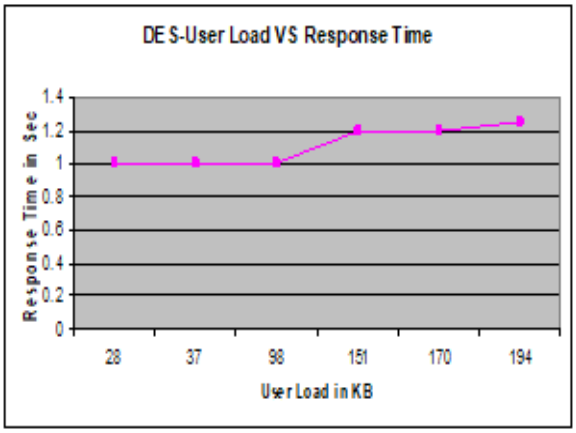


Fig 10 Comparison between user load with response Time for DES

From the performance analysis chart, the DES response is very quick irrespective of the load size. Since this project mainly focuses on securely transmission of voice information on network, the fastest encryption algorithm is preferred. From the above comparison the DES algorithm provides very quick response compare with RSA. Thus, in this project DES algorithm is used for encryption.

VI. CONCLUSION

In general, the Session Initiation Protocol (SIP) is used to locate communicating parties on the Internet. On security concern the existing mechanisms in the Session Initiation Protocol (SIP) are inadequate for cryptographically assuring the identity of the end Users that originate SIP requests. The proposed system defines a SIP header field for Identity. It is verified by a signature and the packet is transmitted after encryption. The reverse process is applied on the receiver side to get the original information. Thus, the hacker intrusion between the communicating parties on the Internet has been completely avoided.

REFERENCES

[1] A Lightweight Scheme for Securely and Reliably Locating SIP Users Lei Kong, Vijay Arvind Balasubramaniyan and Mustaque Ahamad College of Computing Georgia Institute of Technology Atlanta, Georgia 30332. 1-4244-0144-5/06/$20.00 ©2006 IEEE

[2] National Institute of standards and Technology US Department of commerce.

[3] The Session Initiation Protocol (SIP) RFC: 3261

[4] IETF RFC 4474 / RFC4474 Enhancements for Authenticated Identity Management in the Session Initiation Protocol.

[5] Threat Assessment of IP Based Voice Systems Threats to the Reliability and Security of IP Based Voice Systems February 10, 2006.

[6] Assessing the Quality of Voice Communications over Internet Backbones Athena P. Markopoulos, Member, IEEE, Fouad A. Tobago, Fellow, IEEE, and Mansour J. Karma, Member, IEEE.

[7] VoIP Security Assessment: Methods and Tools H. Abdelnur, V. Cridlig, R. State and O. Festor LORIA - INRIA Lorraine 615, rue du jardin botanique 54602 Villers-les-Nancy, France.

[8] Bojovic, Z., Peric, Z., Delic, V., Secerov, E., Secujski, M., & Senk, V, “Comparative Analysis of the Performance of Different Codecs in a Live VoIP Network using SIP Protocol”. Elektronika. Ir.Elektrotechnika, (2012). 117(1), 37-42.

[9] Voice over IP technologies Mark A. Miller, P.E. WILEY dreamtech India Pvt.Ltd.

[10] J. Evers., VOIP security prototype gets an airing, CNET News.com, July 28, 2005.

[11] Stallings, Cryptography & Network Security - Principles & Practice, Prentice Hall, 3rd Edition 2002.

[12] DALLAS MAXIM semiconductor Oct 2002.

[13] JISC Technology and Standards Watch, September 2006.

[14] J. Rosenberg and H. Schulzrinne. Session Initiation Protocol (SIP) Locating SIP servers, RFC 3263, June 2002.

[15] D. Luksa, S. Fajt and M. Krhen, "Sound quality assessment in VOIP environment," 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2014, pp. 1066-1070.