End to End Encryption Architecture for Voice over Internet Protocol

Kaustubh Lohiya
Department of Computer Engineering
Mukesh Patel School of Technology, Management and Engineering
Mumbai-56, India

Narendra Shekokar
Department of Computer Engineering
D.J. Sanghvi College of Engineering
Mumbai-56, India

Satish R. Devane
Department of Computer Engineering
RAIT College

ABSTRACT

Session Initiation Protocol (SIP) is an open standard protocol and constitutes the provisioning of services like Internet Telephony and Instant Messaging. Vulnerabilities in SIP have made it possible to exploit it and launch many of the known internet attacks and also few specific attacks, thus affecting the services deploying SIP for session management. To maintain the confidentiality and integrity of voice data security mechanisms need to be deployed. Currently available security measures do not take into account real time nature of data and are generic i.e. not optimized for VoIP technology. This paper presents new end to end encryption architecture for securing the VoIP calls which use SIP to establish their session taking into account the real time nature of data.

General Terms

SIP Vulnerability, VoIP Security, Threats and attacks, SIP Messages, SIP Communication

Keywords

SIP Vulnerability, Encryption Algorithm, VOIP exploitation, VOIP Communication.

1. INTRODUCTION

Voice over Internet Protocol (VoIP) [1] is a new emerging technology used for voice communication using existing internet infrastructure. The session management in VOIP is done with protocols like H.323 [1], SIP [1][13]. Session initiation protocol is a text based application layer protocol designed to be independent of the underlying layer of TCP/IP model or OSI Model. It is used to create, modify and terminate a session. SIP incorporates many elements and features from Hypertext Transfer Protocol and Simple Mail Transfer Protocol [11]. However this protocol has many known vulnerabilities which can be exploited to launch attacks against VoIP Systems. This paper introduces a new architecture and encryption algorithm to overcome the known vulnerabilities and thus make VoIP more secure than it is presently.

The paper is organized as follow: The section II deals with the existing architecture and call flow setup of SIP. In the section III of the paper we present some of the vulnerabilities and attacks possible on the SIP which affects the VOIP communication especially confidentiality and integrity of the data. The section IV deals with the existing solutions proposed and implemented for securing SIP, also there affects and drawbacks will be analysed. Section V we present our new architecture for session establishment which will support end to end architecture and overcome the drawbacks of existing solutions.

2. EXISTING SIP CALL SETUP

To understand the concept of existing call setup we need to understand a few basic concepts. SIP works on a request-response model where in every request made has an associated response to it [13]. These requests are generated by the sender which can be a client or proxy server. Some of the request messages are as follows

- REGISTER: Used by a UA to indicate its current IP address and the URLs for which it would like to receive calls.
- INVITE: Used to establish a session between user agents.
- CANCEL: Terminates a pending request.
- BYE: Terminates a session between two users.

To each of the above mentioned request message there is a unique response generated and has a particular code (three digits) associated with it. The start of the code (first digit) denotes the kind of action being taken place. Thus for the above request message, response will be generated from the following category of response messages

- Provisional (1xx): Client request received and is under processing.
- Success (2xx): Successfully processed the request sent by client
- Redirection (3xx): Communication needs further assistance form client side
- Client Error (4xx): Invalid request received from client, typically syntax error, unauthorized.
- Server Error (5xx): The server has failed or crashed and hence no valid response can be generated.
- Global Failure (6xx): Entire network might be down and none of the request can be attended

In VOIP communication we have various different network components viz. User Agent Client: End points who communicate with each other and User Agent Server: They and help in establishing the session. User agent server is of following type:

- Proxy Server [1], which acts as both server and client and are responsible for the intermediate request and response generation.
- Registrar Server [1], it accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.
- Redirect Server [1] is a user agent server that generates 3xx responses to requests it receives
- Location Server [1], which gives the actual location of the UAC.

2.1 Session Establishment

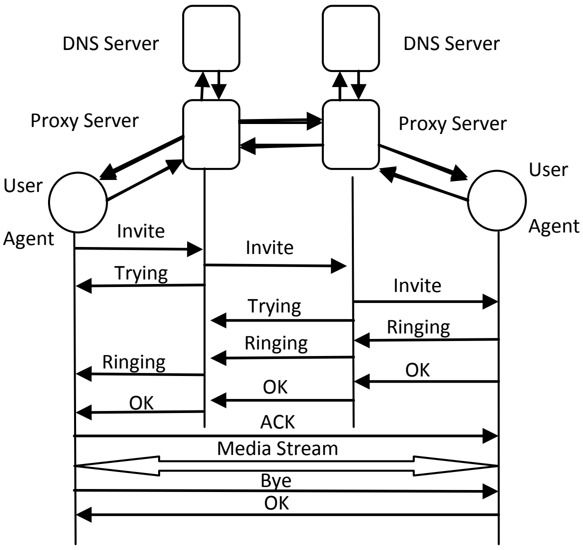

Fig 1: SIP Session Establishment

Figure 1 shows a typical session establishment of using SIP protocol. The Request and Response is shown above and the role of proxy server and DNS and location can be easily made out, the diagram is very self explanatory. Thus As from the diagram if UA-1 wants to communicate with UA-2 then the request message INVITE is generated by UA1 and sent to UA-2 via the proxy servers in between. For every point at proxy a response is generated and sent to previous node.

3. SIP VULNERABILITIES AND ATTACKS

Absence of mutual authentication is seen in most the messages exchanged between proxy and client. This lack of mutual authentication leads to attacks like BYE attack [8][6], Proxy Impersonation [2], Session Tear Down [2] and SIP Cancel Attack [6]. Another major issue is that messages from server to client are sent in plain text format which is very easy to intercept and tamper with, thus leasing to message tampering [2][8] attacks. Also the credential information is not well protected. SIP implies base64 encoding for securing credentials which is a very form of encryption. It can be easily broken and credential information can be used to launch Registrations Hijacking [2] or Deregistration attack and Invite attack. All these vulnerabilities and attacks affect the quality of VoIP call and affect the end user drastically. Thus it is a very important to secure the SIP using an encryption algorithm which can support the real time data flow in VoIP.

3.1 Existing security measures and weakness

The inbuilt security mechanism in the SIP is the digest authentication scheme [3][14] derived from HTTP digest authentication [14]. The digest scheme is based on challenge response mechanism and uses Base-64 encoding for cryptography. SIP digest authentication cannot support message integrity and confidentiality. As the digest authentication involves very weak form of encoding the method is vulnerable to well known plaintext, and man-in-the-middle attacks. Cipher text cannot offer an advanced security level since it is feasible to compute the message credentials by launching a brute force attack on the encrypted password.

Other security measure includes the usage of S/MIME within SIP [5]. MIME itself defines mechanisms for the integrity protection and the encryption of the MIME contents. SIP may use S/MIME to enable mechanisms like public key distribution, authentication and integrity protection, or confidentiality of SIP signalling data. To be able to protect SIP header fields as well, tunnelling of SIP messages in MIME bodies is specified. Generally the proposed SIP tunnelling for SIP header protection will create additional overhead. S/MIME requires certificates and private keys to be used, whereas the certificates may be issued by a trusted third party or may be self-generated. The latter case may not provide real user authentication but may be used to provide a limited form of message integrity protection. On the other hand, the lack of PKI in VoIP does not offer the appropriate environment for the utilization of S/MIME.

Other encryption techniques like TLS [7] and IPSec [5][7] are not ideal of use along with SIP because of high network over head and they have to implemented in Hop-by-Hop fashion causing decrease of efficiency and also opening the packet to a attackers at every hop, Thus not providing a good security measure in VOIP environment. Also the protection offered by IPSec assumes pre-established trust among the communicating parties and it can only be utilized in a hop-by-hop fashion. Since IPSec is implemented at the operating system level, most SIP clients do not implement this protocol yet. For this reason, IPSec can only protect the traffic between the corresponding network servers. Moreover, SIP specifications do not suggest any framework for key administration, which is required by IPSec. In contrast to IPSec, TLS does not assume any trust relation among communicating parties. TLS can be utilized either for one-way or mutual authentication schemes and maybe it is more suitable for inter domain authentication. Of course, there is always the risk that the message can be intercepted inside the recipient’s network if the last hop is not encrypted. Additionally, TLS is used by the SIPS scheme to offer an end-to-end security [7]. However, TLS fails to deliver end-to-end security and protects only connection-oriented protocols.

Thus all the method do not offer end to end encryption standard. The methods are generic and not optimised for VoIP communication and hence generate lot of network overheads which is not acceptable in real time data transmission. Hence we have proposed our own architecture along with the encryption standard which takes into account above factors.

4. PROPOSED ARCHITECTURE

We present a new architecture for VoIP communication which consists of a symmetric key [12] encryption scheme, distribution technique for the key and an architectural design of the network. The encryption scheme will be used to encrypt the entire SIP Message packet except for the “TO” field in the header, the key distribution scheme [9] helps transmit the symmetric key securely which will be used as a session key for later on message exchange. The new proposed architecture helps us to achieve an end to end encryption thus overcoming the draw backs of today's hop-by-hop way of encryption in VoIP.

4.1 Encryption Scheme:

The encryption scheme proposed is a symmetric key block cipher technique. It is based on Feistal cipher technique and derives its base from TEA.

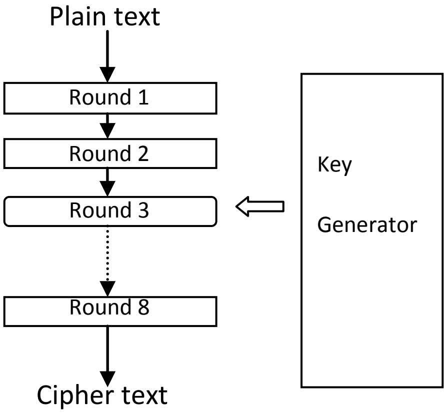

Figure 2: Encryption Scheme

The input text is of 128 bit. 128 bit key is vulnerable to brute force attacks and hence comparatively weak, hence we use a 256 bit key for the encryption. The pain text of 128 bit is divided into blocks of two, each of 64 bit viz. left and right. The right block undergoes transformation based on shift operations, XOR and modulo addition operation however the left block is bought down as it is

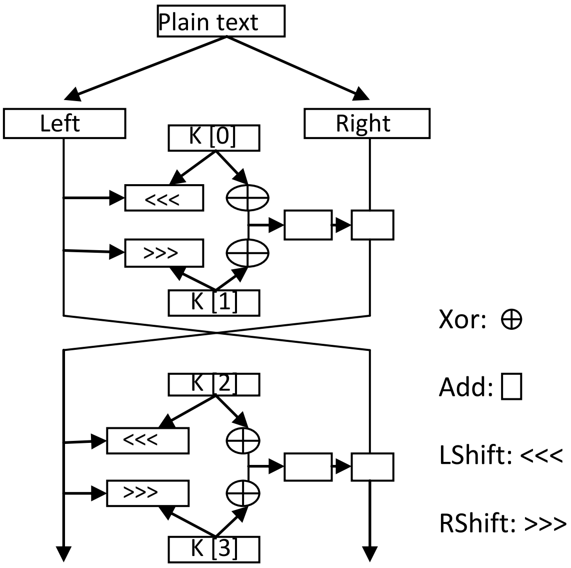

Figure 3: Encryption Cycle

The new intermediate left and right blocks are then interchanged and the round repeats. These 2 rounds make 1 cycle of encryption and we will make use of 8 such cycle to achieve the properties of encryption. The shift operations make use of both left and right shift and the number of shifts is dependent on the key. The plaintext of 128 bit gets split into half viz. left and right. The left block of plain text is then sent to Shift registers viz. left and right. The left shift register performs a left circular shift on the data depending on the first bit of the sub-key K1 and similarly the right circular shift using first bit of sub-key K2. The output of shift registers is then XORed with the respective sub-key K1 and K2. On the outputs we perform a modulus addition to keep the data within specific range of ASCII value. Finally the output of addition is again XORed with 64 bit right data. The left and right intermediate outputs are then exchanged and same process is repeated. 8 such cycles helps to achieve complete diffusion of plaintext.

4.2 Key Exchange:

The Key for the encryption is generated at the side who wants to initiate a connection. The key will is 256 bit and will be used as a session key for further communication throughout the session.

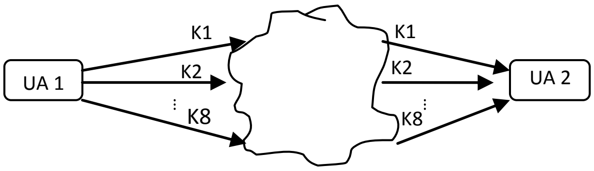

Figure 4: Key exchange

The 256 bit key is divided into blocks of 32 bits. Every block is the routed through the internet cloud and it is suggested that all the 8 blocks of key be routed through different routes [9]. This decreases the probability of a key being compromised.

4.3 The new Architecture

Our new architecture is based on DNS approach [10] and partly takes into account triangular routing. We make use of two types of DNS in our approach

1. Home DNS: This DNS belongs to the home network where the SIP client is first registered.
2. Foreign DNS: This refers to DNS which represent the networks other than the respective home network of the client.

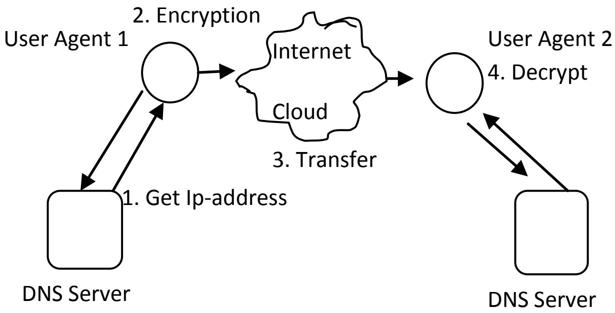

Figure 5: New Architecture

Communication takes place by IP resolution first and then encrypting the entire session packet using our proposed encryption algorithm. Thus the user which want to communicates resolves the IP address of the callee using its home DNS. The IP is globally unique IP and thus the session packet is formed using this IP. All the packet contents are encrypted using the above encryption algorithm except the "To" field. The packet is then sent via the internet cloud to reach its destination and the routing is handled by the intermediate routers. The callee on receiving the packet decrypts the packet using the symmetric key shared.

We make use of statistical data and our approach is based certain assumed facts like caller and callee having a VOIP call mostly know each other like friends, colleagues etc thus the callee has to be present in the address book of caller. Now suppose the callee moves into another network, in this case the callee attaches itself to the new network and it then sends the IP update to its respective Home DNS and the DNS of other network on which it has contacts on, this ensures we generate less no. Of over head as only limited DNS will be updated which callee frequently connects to. Thus any known contact of callee wants to communicate then it will get the IP address from its DNS which has been updated. However if someone not in contact book of callee want to call then the session will be routed through the home DNS that is nothing but triangular routing, thus the request will be sent to the home DNS the home DNS will find the new location of its callee and forward the address to the caller after which the session will be established. In this way we are reducing the network overheads using statistical multiplexing and updating a limited number of DNS. The DNS which are updated have the high probability of contact with the Callee.

Another Scenario to be taken into account is if the caller moves into the new network then we have two options one it keeps its Home DNS as its DNS and uses its home DNS to resolve the IP of the contact it wishes to contact or secondly it can move entries pertaining to its contact from its home DNS to the new DNS where it has moved in. One of the options can be used depending on the factor like if network being moved to is geographical far away , time for which the caller has shifted into the network.

5. CONCLUSION

In this paper we have discussed the weakness of the existing VoIP infrastructure, various vulnerabilities were found out which lead to attacks and hence compromised the security in communication. A new architecture was proposed along with encryption method VoIP taking into account the real time nature of data. The new architecture was designed along with encryption to offer an end to end security in VOIP communication, thus preventing hackers from intercepting VOIP sessions. The proposed technique mitigates many VOIP attacks without introducing much delay or overheads in communication. The architecture is being implemented nad tested in windows environment and needs to be evaluated further and finely tuned to create a safer real world VoIP environment.

6. ACKNOWLEDGMENTS

Our special thanks to our friends who have constantly inspired us and their constant feedback has made possible this research and paper. Our heartiest gratitude to our family members, without their support, understanding and patience this would not have been possible.

7. REFERENCES

[1] H. Abdelmr, R. State, I. Chrisment, C. Popi, "Assessing the security of VoIP Services" IEEE 2007 paper 1-4244-0799-0/07.

[2] Liancheng Shan and Ning Jiang, "Research on Security Mechanisms of SIP-based VoIP System" IEEE 2009 paper 978-0-7695-3745-0/09.

[3] Valentina Casola, Massimiliano Rak, Antonino Mazzeo, Nicola Mazzoccca, "Security Design and Evaluation in a VoIP Secure Infrastracture: A Policy Based Approach" in ITCC 2005, paper 0-7695-2315-3/05

[4] Moses Garuba, Jiang Li and Zhenqiang Yi, "Security in the Era of Telecommunication: Threats, Risks and Control of VoIP" IEEE 2008, paper 978-0-7695-3099-4/08.

[5] Dimitris Geneiatakis, Tasos Dagiuklas, Georgios Kambourakis, Costas Lambrinoudakis, Stefanos Gritzalis, "Survey of Security Vulnerabilites in Session Initiation Protocol" IEEE Communication Surveys, Volume 8, No.3, pp 1553-877X , 2006.

[6] Housam Al-Allouni1 Alaa Eldin Rohiem Mohammed Hashem Ali El-moghazy Abd El Aziz Ahmed "VoIP Denial of Service Attacks Classification and Implementation" in NRSC 2009, paper C14-1.

[7] Wafaa Bou Diab, Samir Tohme, carole Bassil, "VPN Analysis and New Perspective for Securing Voice over VPN Networks" in Networking and Services IEEE conference 2008, paper 0-7695-3094-X/08.

[8] David Butcher, Xiangyang Li, Jinhua Guo, "Security Challenge and Defense in VoIP Infrastructures" IEEE Transaction on System, Man and Cybernetics-Part C, Volume 37, No 6, pp 1094-6977, 2007

[9] Arno Wacker, Mirko Knoll, Timo Heiber and Kurt Rothermel, "A new Approach for establishing Pairwise keys for Securing Wireless Networks" in SenSys internal Conference 2005, paper 1-59593-054-X/05/0011

[10] Alex C, Snoeren and Hari Balakrishnan, "An End-to-End Approach to Host Mobility" in IEEE International Conference MobiCom 2000, paper 2000-08/2000.

[11] Chan Yeob Yeun, Salman Mohammed Al-Marzouqi, "Practical Implementations for Securing VoIP Enabled Mobile Devices" in Third IEEE international conference on Network and System Security 2009, paper 978-0-7695-3838-9/09.

[12] Behrouz A. Forouzan, Cryptography and Network Securit, Special Indian Edition, 2007.

[13] SIP: Session Initiation Protocol, IETF RFC 3261, 2002.

[14] Digest Access Authentication, IETF RFC 2069, 1997.

[15] Prateek Gupta, Vitaly Shmatikov, "Security Analysis of Voice-over-IP Protocols" in conference, paper 0-7695-2819-8/07.