INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Secure 2-Way Authentication for SIP

Mihir Nanavati[1], Imaad Ukaye[2], Miraj Shah[3]

[1]Dwarkadas J. Sanghvi College of Engineering,
Vile Parle, Mumbai, India
nanavati93@gmail.com

[2]Dwarkadas J. Sanghvi College of Engineering,
Vile Parle, Mumbai, India
imaad.ukaye@gmail.com

[3]Dwarkadas J. Sanghvi College of Engineering,
Vile Parle, Mumbai, India
mirajshah05@hotmail.com

Abstract— *In recent years, Session Initiation Protocol (SIP) has become widely used in current internet protocols to control media communication sessions. It is a text-based application control protocol much like Hyper Text Transport Protocol (HTTP) and Simple Mail Transport Protocol (SMTP) and is a strong signaling protocol on the internet for establishment, maintenance, and termination of media sessions. This paper presents some threats and attacks that SIP is vulnerable to and suggests a solution which can overcome these security loopholes and provide a secure communication over the unsecured network. There are basically three security considerations that need to be reckoned, namely Integrity, Authentication and Confidentiality amongst which we have tried to strengthen the Authentication scheme. The respective existing solutions are highlighted and several other challenges are identified. We have proposed a solution that can improve the security of SIP by using the concept of session keys generated randomly during communication along with the use of public key cryptography as against only symmetric key cryptography which is easily breakable, to further strengthen VoIP communication.*

Keywords: *SIP attack, handshake, authentication, VoIP, asymmetric key*

1. INTRODUCTION

The Internet Engineering Task Force (IETF) proposed the Session Initiation Protocol (SIP) [1] as the IP-based telephony protocol. SIP seems to be the most promising candidate for call setup signaling for future IP-based telephony services, and it has been chosen by the Third-Generation Partnership Project (3GPP)[8] as the protocol for multimedia application in 3G mobile networks. SIP has recently become the main signaling protocol for Internet applications, thus allowing the implementation of a number of features using SIP, such as video conferencing, online gaming, peer-to-peer application, instant messaging, presence services and voicemail. Hotline services for emergency calls and online flight booking also use SIP. SIP also supports mobile applications, which are more flexible applications than others. SIP is implemented in different wired and wireless networks, which has security issues. Although SIP has been widely deployed, the study of SIP security is still immature. So it is important to look into security problems and solutions for SIP-based networks.

The security issues of SIP have been investigated a great deal [3-4][10]. Despite the diverse security mechanisms that have been proposed for SIP-based infrastructures [1], there are still vulnerabilities that affect this architecture. Such vulnerabilities aim to exhaust available resources, create false responses upon the reception of malicious requests, and discover possible security vulnerabilities in the applications.

2. SIP ARHITECTURE

SIP is an application-layer signaling protocol [1] for handling multimedia sessions over the Internet. The IETF defined a protocol designed specifically for the control of real-time multimedia communications. The intention is not to limit the requirements to support voice, but to create a specific session control protocol capable of supporting all forms of communications. VoIP protocol deployment has several versions. SIP is one of the most studied protocols because of its ability to support multiple media types. In a typical SIP-based network infrastructure, the following network elements are involved [12]:

• User Agents: user agents (UAs) act on behalf of an end user terminal. A user agent client (UAC) is responsible to create requests and a user agent server (UAS) processes and responds to each request generated by a UAC.

• Registrar: UAs contact registrar servers to announce their presence in the network. The SIP registrar server is a database containing locations as well as user preferences as indicated by the UAs.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

• Proxy: A proxy server receives a request and forwards it towards the current location of the callee — either directly to the callee or to another server that might be better informed about the actual location of the callee.

• Redirect: A redirect server receives a request and informs the caller's UA about the next hop server. The caller's UA then contacts the next hop server directly.

The protocol was derived from Hypertext Transfer Protocol (HTTP); several aspects of SIP protocol resemble HTTP. SIP is also implemented in web services and e-mail. A full SIP URI (Uniform Resource Identifier) is shown as: SIP URI = SIP username@ (IP or domain). SIP is text-based, which makes it simpler to understand than most bit-oriented protocols, where knowledge of the significance of each bit position according to the rules and syntax of the defined protocol is required. The Transport of SIP messages can be carried by transport-layer over IP protocols, such as SIP over UDP or TCP.

3. SIP ATTACKS

SIP suffers from various types of attacks and vulnerabilities mainly due to the utilization of an open environment like Internet. The major problem with the SIP authentication method is the use of HTTP Authentication [2].It is a very weak authentication method whereby in Basic mode the User-Name: Password key-value pair is sent in clear text. Although in Digest mode, password is encrypted but it is not at all sufficient. These packets can be intercepted by intruder and can be easily replayed. Also as intruder clearly intercept the password although in encrypted form, it won't take much time for him to break the password through dictionary attack and as the same password will be used in the next session the intruder can easily morph the server with the legitimate users identity[11].

Here we list the attacks that can be performed on SIP based application quite easily [7].

- Replay Attack
- Registration Hijacking(MiM)
- Request Intercepting and Spoofing
- Impersonating a Server
- Plaintext Attack.
- Denial of Service (DoS).

Due to the lack of strong encryption algorithm, various VOIP applications like *Skype* had become victims of various attacks [9]. Registration Hijacking and Server impersonification has become the most common attacks for SIP. Below we illustrate the results of the experiments done by us. We intercepted a VOIP call and tried to decode it using ordinary packet tracer software. Figure 1 clearly exhibit the sequence of packets sent and received by the sender and receiver along with their IP addresses and timestamp. We also decoded all the audio packets and the conversation was clearly audible. The graph of the conversation is shown in Figure 2.

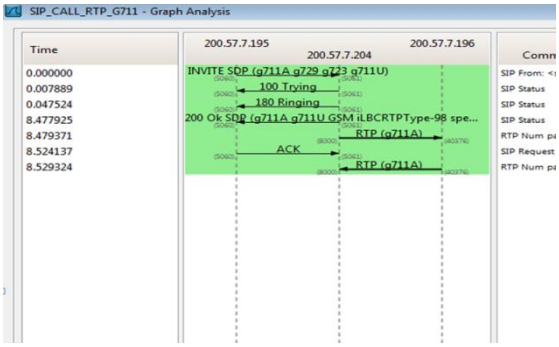

Figure 1: VOIP call Flow-graph.

Thus, even without the application of sophisticated intercepting software of VOIP, SIP based packets are very easy to crack if complex handshaking is not used.

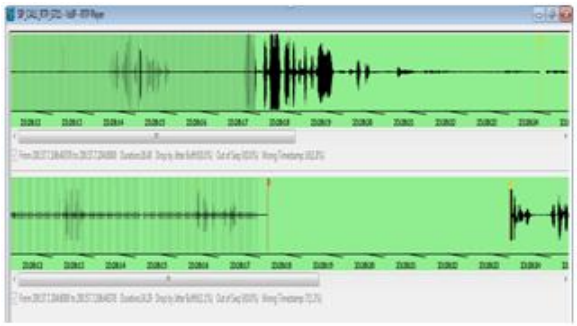

Figure 2: VOIP call.

So, we tried to analyze the flaws in plain SIP protocol from security point of view and found the following results [6] [13]:

- There is a requirement for authentication that is two way. This is important because the Man in Middle may mislead client to steal his credential. It may also deceive server for using services entitled to some other user.
- The use of plain text (even in Digest authentication only password is encrypted) makes it very easy for the intruder to intercept the messages and thus confidentiality of the message is not assured. So, there is a very basic requirement to encrypt the complete messages using some key.
- Use of the nonce which is set as recommended [1] must be made mandatory. It should also be encrypted with the message. This will avoid the replay attack.
- The key used in the encryption and decryption should not remain same for all the session. If the key remains same the interceptor may apply dictionary attack and may decode the message acquiring the key.

4. PROPOSED SOLUTION

Encryption of the packet is an essential part for maintaining the integrity of the data. So, we can encrypt the packets by making use of symmetric key as well as asymmetric key cryptography. Each of these techniques has its own set of advantage and disadvantages. Symmetric key is simple and fast. But it uses same key on

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

both sides. So once key is identified whole communication can be decrypted. On the other hand Asymmetric keys are difficult to crack. As they are difficult to compute, they require more time than symmetric key and are slower. So in the solution we propose to make use of both the cryptographic techniques to their advantage. We use asymmetric key for generation of session key and then this session key is symmetric key which will be used throughout the session and new session key will be generated for every session. Although TLS based solutions have been proposed but they are found to be inadequate.[5] We next explain our approach in more detailed manner.

Let's make a quick note of the attacks which will be avoided by using the following message format in SIP

- Session hijacking.
- Registration hijacking.
- MiM.
- DOS.
- Message tampering.
- Message sniffing.
- Replay attack,

The given text is presented as a scenario wherein ALICE(remote user) wants to start a new session with BOB(server). Alice will need to provide her credential information to BOB to start a session. Trudy is the intruder who is trying to intercept and tamper the messages. We will note few symbols that will be used in further text in Table 1.

Symbol	Description
$\{\ \}_x$	Public key of x
$[\ ]_x$	Private key of x
k_{AB}	Session Key
RS	System generated Random String.

Table 1: Symbols

4.1. REGISTER MESSAGE:-

Here ALICE and BOB communicate to each other through unsecured communication line as shown in Figure 3. Making use of public key infrastructure ALICE sends the Registration request to BOB using the public key of BOB. Along with the Registration message, ALICE also sends her password and a Random string (RS_1) which will be used for mutual authentication between ALICE and BOB. As the message is encrypted by the public key of BOB, it can only be decrypted by BOB's private key.

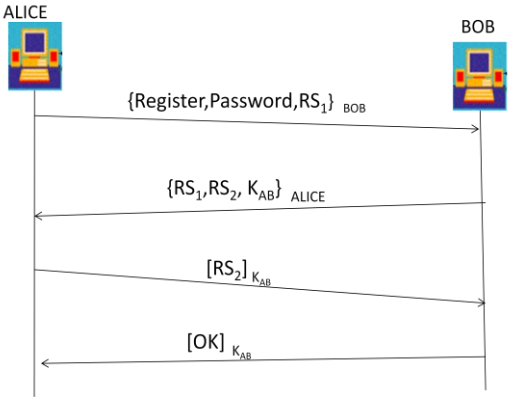

Figure 3: Register Message

Now considering BOB has decrypted the message using his private key, he can authenticate ALICE by matching her password with the one stored in database but still he is not sure of sender's identity as it could be just a replay of previously intercepted message. Now, BOB will generate a new packet that will contain the Random string (RS_1) sent by ALICE, a new Random string (RS_2) and a session key (K_{AB}) generated by BOB that will be used by both the parties to communicate if the registration process is successful. BOB sends this packet to ALICE by encrypting it with public key of ALICE which can only be decrypted by ALICE's private key.

Now ALICE will decrypt the message using her private key and recover the message which contains the two random strings. The packet contains the random string (RS_1) sent by Alice which authenticates BOB's identity. ALICE will now send the random string RS_2 received in the message generated by BOB. Now, ALICE will encrypt the message using the symmetric key (K_{AB}) sent to her by BOB. Once BOB receive this message he will decrypt it using the Symmetric Key K_{AB} i.e. the session key. If the random string is correct then BOB will send Ok message to ALICE again encrypting it with session key indicating the authentication process has been successful and the session has been initialized. Using this OK message BOB indicates to ALICE that all further communication will be done using the generated symmetric key. But in case the connection couldn't be setup then BOB will send a CANCEL message to ALICE.

Now moving on to Registration Hijacking attacks which takes place in the traditional SIP protocol but avoided in our proposed solution. Registration Hijacking is avoided even if the Trudy is able to find username and password of the legitimate user or just by replaying the intercepted messages, he wouldn't be able to complete the registration process as he doesn't know the private key of Alice and so he could not sent RS_2 back to BOB. So, BOB will not initialize the session. Also Man-in-Middle (MiM) attack will be avoided. In this attack Trudy will impersonate a legitimate server and will try to leverage all the possible information for its user. This will be avoided as Trudy will have to revert back to Alice by a message with RS_1 in it. And to know RS_1 Trudy must be able to decrypt the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

message received from Alice which is encrypted using public key of Bob and hence must have information about private key of Bob which is unknown to him. Thus, we have developed a two way authentication protocol where both Alice and Bob authenticate each other.

4.2. CANCEL MESSAGE

Cancel Message is used in SIP for cancelling the incoming call or rejecting a request. This message is also used by attackers for rejecting the incoming request. If the attackers get hold of intermediate proxy, attacker rejects all the incoming requests thus leading to Denial of Service to legitimate user.

In accordance with the Register message described above, Alice will send a Register message to BOB using the public key of BOB. Now say Bob is not in position to answer the call then Bob will reject the call. For rejecting the call, Bob will not send a plan text cancel message instead it will send a message consisting of Random String (RS1) along will nonce and encrypt it using public key of Alice as shown in Figure 4. So, decrypting this message Alice will recover the Random String (RS1) which confirms that the Cancel message is from BOB and is not a DoS attack and it will terminate the request and if required retry later.

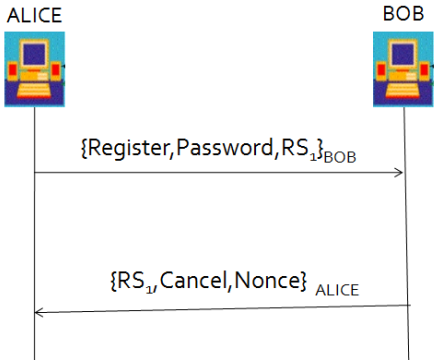

Figure 4: Cancel Message

Now, above method of cancelling a request reduces possibility of Denial of Service Attack (DoS). In the traditional SIP, attacker used to send random CANCEL messages to the legitimate users and use to end their sessions abruptly. So as the packet is encrypted by public keys of recipient, the interception and decryption of packets is very difficult. Also, as attacker has to send RS1 (challenge) back to Alice (sender) which can only be known by its original recipient DoS attack is avoided.

4.3. DATA MESSAGE:-

Now to avoid the data messages from being intercepted and tampered we will use encryption. Here all the data transfer between BOB and ALICE will take place using the Symmetric key (KAB) generated during the registration process.

When ALICE wishes to send some data to BOB, she will send the message along with the nonce to BOB encrypted with the session key as shown in Figure 5. Now BOB will decrypt it and check if the nonce value is within certain threshold then the packet will be accepted, else it will be discarded. Similar procedure will be repeated when BOB sends some data to ALICE.

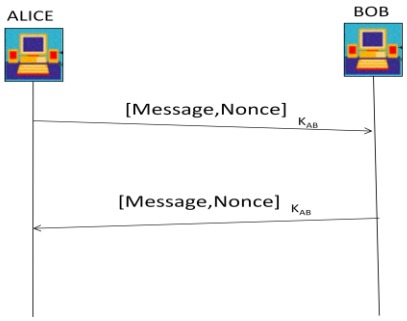

Figure 5: Data Message

By using this procedure Trudy cannot send any messages to either Alice or Bob as he/she is not aware of the session key. So the possibility of messages being tampered is ruled out. Also, Trudy cannot resend messages by intercepting them as each message contains nonce which is similar to timestamp and hence if the nonce value is older than the allowable threshold it will be discarded.

4.4. BYE MESSAGE:

BYE is another popular message among the attacker as it is one of the most vulnerable and an easy tool for launching a Denial of Service attack (DoS).In SIP, Bye message is used for terminating the session. Attacker simply sends the Bye message to User Agent communicating with the server and terminates the session thus depriving user from the services. This is one form of Denial of Service Attack.

Now to avoid such abrupt session teardown we use a procedure whereby if ALICE want to send a Bye message to BOB she will encrypt it with the session key as shown in Figure 6. Also along with Bye message a nonce will be send. Now BOB will decrypt it and check the nonce value, if nonce is within certain threshold then the packet will be accepted and similarly Bye message will be sent from BOB to ALICE. Similar process can be followed by BOB if it wants to terminate the session.

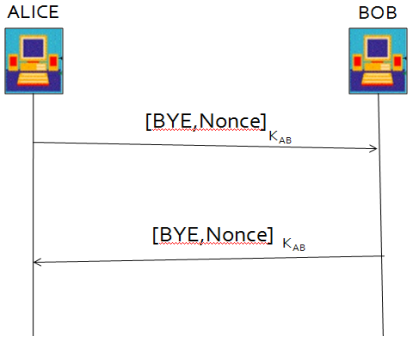

Figure 6: Bye Message

Use of this procedure reduces the possibility of Denial of Service Attack (DoS).Now as the messages needs to be encrypted with the session key it can be sent by only nodes that are aware of the session key. Also replay attack is avoided as the message now contains nonce.

5. PROS AND CONS OF SUGGESTED SOLUTION

New Session key is generated for every session and by using sufficiently long key (128-bit or longer) for encryption the strength of the authentication method can be increased. Also, by using Asymmetric key cryptography it may take decades for intruder to compute the key. Even if attacker gets the knowledge about the key it may not be useful for next session. Supposedly, the control of user computer is received then also the keys of communication can't be obtained as session keys are not stored anywhere they are discarded once the session is tear down and are newly generated by the Registration process of every session.

More secure than existing system (SSL) as apart from just using Digital Certificate, a two-way authentication Challenge Response stage is included. All conventional attacks can be avoided as explained in each of the respective sections. Hence, it is much better security then SIP's Digest Authentication.

Cost of Public Key Encryption's has high computational cost. Incurring to the cost of Digital Certificates as they have to be purchased from the Certificate Authority (CA), more complex mechanism of communication has to be incurred. But to limit the computational time to minimum we make use of public key cryptography only during the registration process. We make use of symmetric key cryptography during data transfer to make the signaling process fast. After considering the overall security provided by the suggested method, pros outweigh the cons.

6. CONCLUSION

IP is not an easy signaling protocol to secure. A discussion for solutions to SIP based security malfunctions consisting of implementations and simulations are presented in this study. A number of studies were reviewed and some common problems in these methods were identified. A new security mechanism is proposed which overcomes most of the security issues in current SIP implementation. The proposed implementation is based on the use of both public key as well as private key cryptography with a new session key for each session. We propose the use of asymmetric key cryptography in session registration process. Also the message flow sequence and the attacks avoided by this mechanism are proposed in this study.

REFERENCES

[1] J. Rosenberg et al., "Sip: Session Initiation Protocol," RFC 3261, June 2002

[2] J. Franks, P Hallam , "Http Authentication ",RFC 2617,June 1999

[3] Peterson, J. A Privacy Mechanism for the Session Initiation Protocol (SIP). RFC 3323, IETF Network Working Group, November 2002. Online, referred to March 19th 2003.
URL: http://www.ietf.org/rfc/rfc3323.txt

[4] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A. and A. Haukka.. Security Mechanism Agreement for the Session Initiation Protocol (SIP). RFC 3329, IETF Network Working Group, January 2003. Online, referred to March 19th 2003. URL: http://www.ietf.org/rfc/rfc3329.txt

[5] Kazi. and Hoshino. (2008) "TLS Handshake Method based on SIP".

[6] Jan Seedorf ,IEEE Networks,2006

[7] Mark Collier et al 2005

[8] Stefano Salsano , IEEE ,2002

[9] Angelo Keromytis. (2012) "A Comprehensive Survey of VOIP security". IEEE Communication Survey and Tutorials Vol-14., no. 2.

[10] Geneiatakis, D. "SIP Security Mechanism".

[11] McGann , Sicker "An Analysis of Security Threats and Tools in SIP-Based VoIP System".

[12] Aws Naser Jaber, Chen-Wei Tan ,2012

[13] Geneiatakis et al 2006, Sisalem et al 2009, Werapun et al 2009, Zhang 2007