SIP Security Mechanism Techniques on Voice over Internet Protocol (VoIP) System

Ruhul Islam[1], Smarajit Ghosh[2]

[1]*Sikkim Manipal Institute of Technology, Majitar, Rangpo, East Sikkim-737136*

[2]*Thapar University, Patiala-147004, Punjab*

[1]md_ruhul@rediffmail.com

[2]smarajitghosh@rediffmail.com

***Abstract*- SIP-based VoIP system has many security problems because of the security mechanism of VoIP system and other external factors. These effects relate to the following three aspects: confidentiality, integrity and availability. The sip security mechanism technique on VoIP system and the components of SIP have been analyzed in this paper. The attacks on the SIP system, such as the registration hijacking, impersonating a proxy, denial of service and spam are discussed in detail. This paper has also pointed out the insufficiency of the SIP security mechanism, including different types of attacks.**

***Keywords*— VoIP, SIP, UAS, DoS attack, Message Tempering.**

I. INTRODUCTION

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

A. Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports `presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration (as in figure 1). SIP was also designed to avoid the heavy overhead of H.323.

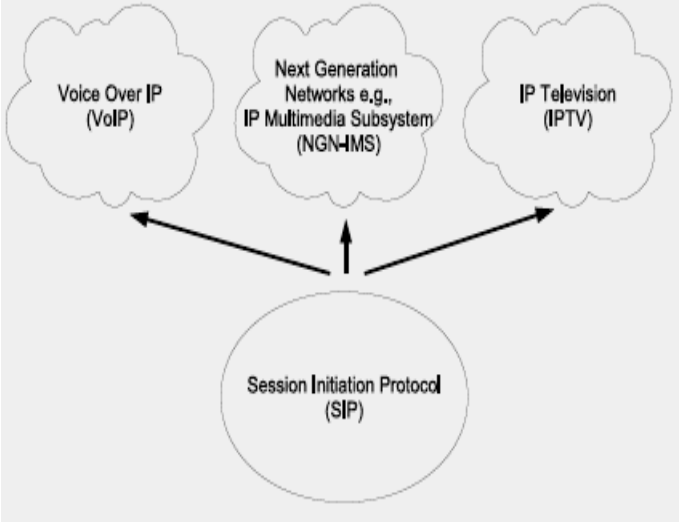

Fig 1: SIP is the basis of most feature IP Communication networks [4]

B. SIP Architecture

Session Initiation Protocol (SIP) is a signalling protocol that can be used in VoIP domain.
The main functions that SIP is designed to support are the following:

1) User location: The aim of user location is to locate the different SIP users in the VoIP domain. Therefore, the SIP protocol can forward any session requests to the destined users. This means a user can use more than one device. Like, more than one user can use one device simultaneously.

2) User availability: In addition to the location of the user, the protocol needs to determine the status of the users whether the user is able to involve in any connections. For example, if the user is busy with

another call, the protocol does not forward the request to the user.

3) User capabilities: This feature performs the different session-related aspects such as the establishment of the connection, the session parameters agreement, and so on.

4) Session setup: In this stage the connection is established between the users. The protocol considers the different parameters in creating the connection.

5) Session management: This functionality of SIP enables the users to modify the session parameters, invoke additional services, and terminate the established connection. The syntax of SIP addresses is similar to that is used in email service. That is, the SIP URL (Uniform Resource Locator) shows two distinct pieces of information. The first part of information that SIP URI reveals is the domain that the user is using at the time of contacting SIP servers. The second piece of information that is shown in SIP URI is either the host name of the computer that is being used by the user or the telephone number of the user's phone.

II. SIP COMPONENTS

A SIP network is composed of the following logical entities: User Agent (UA) -Initiates, receives and terminates calls. Proxy Server - A Proxy Server can requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.

- Redirect Server - Responds to request but does not forward requests.
- Registration Server - Handles UA authentication and registration.

The main components of SIP architecture are User Agent (UA) and SIP server. Figure 2 depicts the main components of SIP architecture. User agents represent the end points or devices that are used by the end users, computers, or VoIP phones. Besides, user agent in SIP has two types based on its role in the communication. The first type is called User Agent Client (UAC) and the other type is User Agent Server (UAS). The basic role of the UAC is to initiate the session request on behalf of the end user. The UAS is use to receives the session request which was initiated by the UAC and responds to this request. So user agent is a mandatory entity in any communication between two users.

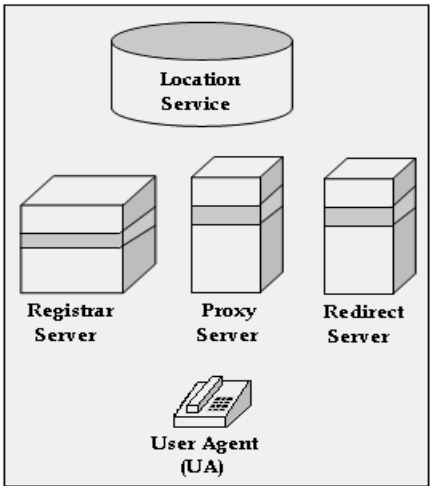

Fig 2: Main components of SIP architecture[2]

III. SECURITY THREATS OF SIP SYSTEM

A. *Registration Hijacking*

Registration hijacking occurs when an attacker impersonates a valid UA to a registrar and replaces the legitimate registration with its own address. This attack causes all incoming calls to be sent to the USER AGENT registered by the attacker. The following figure 3 illustrates registration hijacking:

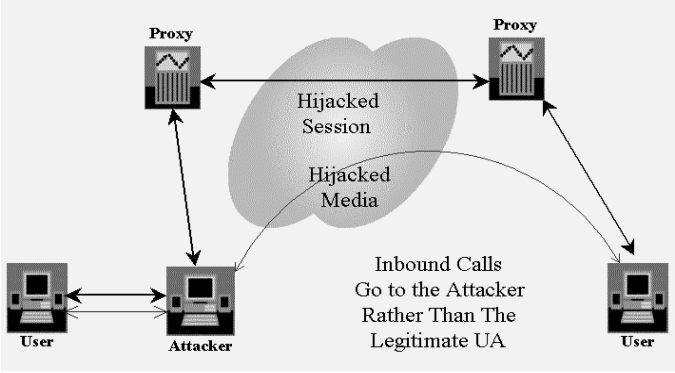

Fig 3: Registration hijacking process on SIP based IP network[11]

Registration is normally performed using UDP, which makes it easier to spoof requests. Authentication is not required and if present, is often weak (just username and password). According to RFC 3261,registrars are only "RECOMMENDED" to challenge registration requests. Most registrars either do not challenge requests, or only require a simple username/password, which can be attacked by dictionary-style attacks. In dictionary-style attack , the attacker has one of your usernames and then steps through a list of likely passwords built based on their knowledge of your enterprise.

An external attacker can build a directory by scanning for your registrable USER AGENT addresses. He can build a list of extensions and use the SIP "OPTIONS" message to covertly build a directory of your users. Some enterprises may use shared, weak, or "mechanically" generated passwords (such as the extension with an extra word). In these cases, an attacker may learns of your passwords. Failed registrations are not always logged. Your SIP proxy will not normally detect directory scanning and registration hijacking attempts. Registration hijacking can result in loss of calls to the legitimate UA, which may be one of your users phones or a critical resource (e.g., a media gateway, Automated Attendant (AA), Interactive Voice Response (IVR), or VM system). Also, the UA can collect authentication or other key signaling information. Or the rogue UA can pose as a Voice Mail system and trick the caller into leaving a message. The rogue UA can also perform a Man-In--Middle (MIML) attack, where it transparently sits between the calling and called UAs, able to collect and modify both the signaling and media. Another type of MIML attack involves redirection of an incoming call to a media gateway, generating toll fraud.

B. *Proxy Impersonation*

Proxy impersonation occurs when an attacker tricks one of your SIP USER AGENT'S or proxies into communicating with a rogue proxy. If an attacker successfully impersonates a proxy, he has access to all SIP messages and is in complete control of the call. The following figure 4 illustrates proxy impersonation:

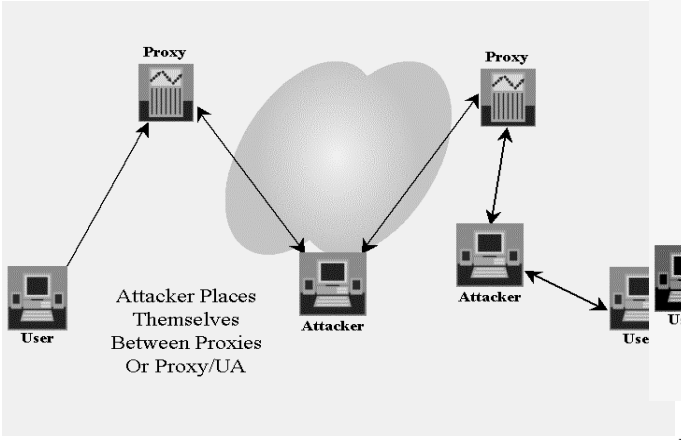

Fig 4: Proxy impersonation attack process on SIP based IP network [11]

Your UAs and proxies normally communicate using UDP and do not require strong authentication to communicate with another proxy. A rogue proxy can therefore insert itself into the signaling stream through several means, including Domain Name Service (DNS) spoofing, Address Resolution Protocol (ARP) cache spoofing, and simply changing the proxy address for a SIP phone. An impersonated proxy has full control over calls and can execute the same types of attacks described for registration hijacking.

If DNS spoofing is used to redirect outgoing calls to a particular domain (e.g., "company.com"), all outbound calls to that site can be intercepted, manipulated, blocked, conferenced or recorded.

ARP cache spoofing is an attack against a network switch that can trick a UA into communicating with a rogue proxy on the internal network. If successful, calls originating from the UA can be intercepted, manipulated, blocked, conferenced, or recorded.

C. *Message Tampering*

Message tampering occurs when an attacker intercepts and modifies packets exchanged between SIP components. Message tampering can occur through registration hijacking, proxy impersonation, or an attack on any component trusted to process SIP messages, such as your proxy, media gateway, or firewall. The following figure 5 illustrates message tampering. SIP messages have no built-in means to insure integrity. By manipulating SIP messages, an attacker can execute the same types of attacks described for registration hijacking and proxy impersonation.

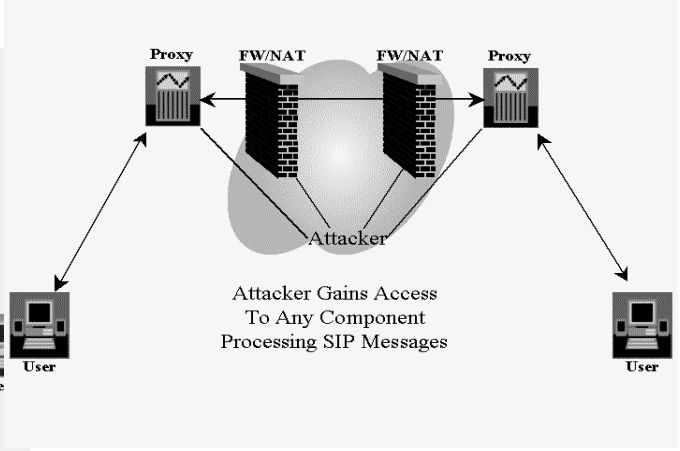

Fig 5: Message tampering process on SIP based IP network[11]

D. *Session Tear Down*

Session tear down occurs when an attacker observes the signaling for a call, and then sends spoofed SIP "BYE" messages to the participating UAs. Most SIP UAs do not require strong authentication, which allows an attacker to send a properly crafted

BYE messages to the two UAs, tearing down the call. The following figure 6 illustrates session tear down:

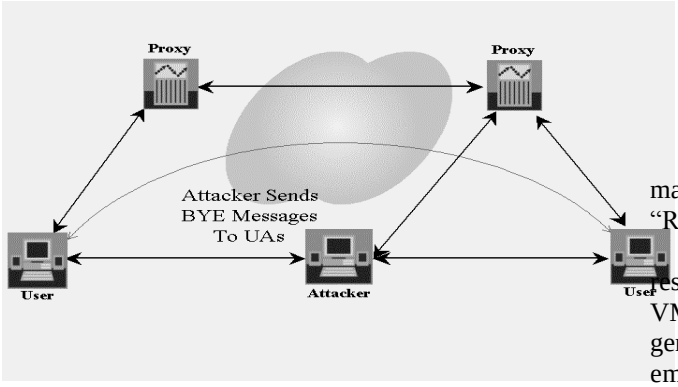

Fig 6: Session tear down occur on SIP based IP network[11]

If a UA does not check the available packet values, the attacker may not even need to observe the call signaling. If the attacker knows the address of a continually active UA (such as your media gateway, AA, IVR, trading floor phone, etc.), they can send BYE messages, causing the call(s) to be torn down. Another example of message tear down is flooding the firewall with BYE messages, possibly tearing down UDP ports opened for legitimate calls.

Denial of Service (DoS) is the primary effect of session tear down. Specific-user DoS or wholesale DoS can occur, depending upon the target. A side effect of session tear down is that the proxy may not be aware of the calls being town down and will not have proper call records.

SIP "RE-INVITE" messages can also be used to modify media sessions. Redirecting media to broadcast addresses can cause a DoS attack. Redirecting media sessions to a media gateway can cause a DoS attack.

E. Denial of Service (DoS)

DoS against a SIP system can occur through any of the means described above or through additional DoS-specific attacks. Because strong authentication is rarely used, SIP processing components must trust and process SIP messages from possible attackers. The following figure 7 illustrates some of the components vulnerable to DoS:

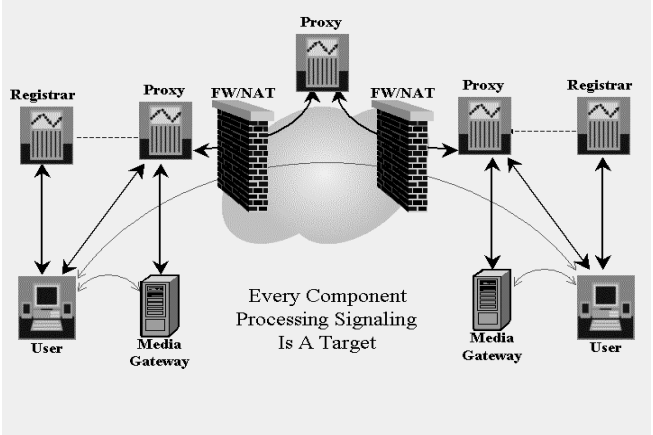

Fig 7: DoS attack process on SIP based IP network[11]

DoS can take the form of malformed packets, manipulating SIP states, and simple flooding, such as a "REGISTER" or "INVITE" storm (a flood of packets).

DoS can be especially damaging if your key voice resources are targeted (e.g., media gateways, AA, IVR, VM, and other systems). DoS can also be used to generate large numbers of toll, information (411), or emergency calls (911). Your network can also be used as a DoS launching point, from which the generated calls are directed at another enterprise.

DoS can also be directed at a firewall. SIP requires management of UDP ports for media. A DoS attack that floods the firewall with calls can prevent it from properly managing ports for legitimate calls.

F. Firewall/Network Address Translation (NAT) Issues

Firewalls are commonly used to protect your trusted network from the Internet or other non trustful network. Data firewalls generally operate at the IP and UDP/TCP layers, determining what types of traffic are allowed and which systems are allowed to communicate. Data firewalls do not typically monitor the application layer – other products, such as an email content monitor or web firewall is used. Data firewalls also create issues for SIP, which uses separate IP ports for signaling and media. SIP embeds media port addresses in the SDP, which the firewall must understand in order to perform SIP-aware NAT (RFC 2993). These and other issues create the need for SIP-optimized firewalls, as shown in figure 8.

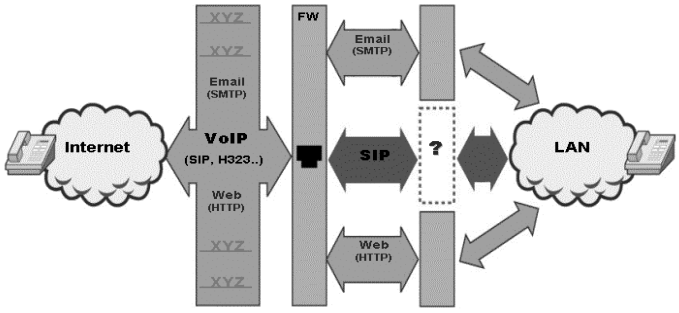

Fig 8: Optimized firewall on SIP based IP network[11]

NAT is commonly used to preserve IP addresses. For SIP to function through a firewall, the NAT must be SIP-aware, in order to modify SIP messages and to control the opening and closing of UDP ports used for media. In the future, if signaling encryption becomes commonly used, in order to function, the NAT must be able to decrypt/re-encrypt the SIP messages.

G. SIP Spam

Spam refers to unsolicited, was forced to accept the information, in the SIP system is called the information received the call, IM or illegal presence information. SIP Spam can be divided into three types [5]: Call Spam, IM Spam and Presence Spam. Spam will bring great harm. First of all, Spam message will contain a virus, resulting in the spread of the virus; Secondly, Spam will reduce the prevalence of SIP system reliability, trustworthiness, the development of SIP adverse effects.

IV. SIP SECURITY MEASURES

SIP employs some security measures to protect the communication between its users, these security measures are not enough to provide the acceptable level of protection to the VoIP service. One of the security measures that SIP utilizes is called Digest authentication. Digest Authentication is a challenge-response HTTP-like authentication. It means that, if a UA or proxy receives a request from another UA, the receiver of the request initiates a challenge asking to the initiator to verify its identity. Although, one of the limitations of Digest authentication is that, it is limited to user-to-user or user-to-proxy communications, but it is not applicable for server-to-server communication. Another limitation of Digest authentication is its unable to protect the confidentiality and integrity of communication. Digest only protects against re-play and illegal access attacks. Because Digest authentication adds timestamp and nonce parameters that show the receiver the creation time of this message. One of these supportive protocols is called S/MIME. S/MIME, stands for Secure/ Multipurpose. Internet Mail Extensions, is a protocol used to secure the confidentiality and integrity of SIP message body of MIME type. The application of S/MIME to the body of SIP message provides the security services: authentication, message body integrity and confidentiality. S/MIME utilizes digital signatures and encryption mechanisms to protect both the integrity and confidentiality of SIP message body. On the other side, S/MIME requires utilization of certificates along with keys. This operation happned only the presence of a key exchange mechanism in the structure of SIP. IPsec provides the ability to use any method of authentication including pre-shared, public/private or Diffie-Hellman keys. In addition to user authentication, IPsec protects the integrity and confidentiality of data by applying hashing and encryption mechanisms. IPsec protects against re-play and repudiation attacks. On the other hand, IPsec has a number of drawbacks such as high overhead production, non-scalability and NAT traversal problem. Another security protocol that can be used in VoIP domain to increase VoIP security level is TLS (Transport Layer Security). TLS protocol belongs to layer 4 of the OSI stack.TLS protects the confidentiality and integrity of communication, it is applicable only for connection-oriented communications, e.g. TCP and SCTP. This restriction limits on TLS across the entire VoIP network if UDP is implemented in some parts of the network. SRTP protocol can be used to secure the real voice communication between the end users. The main protocol that is utilized to carry the voice traffic is RTP (Real Time Protocol). SRTP, which stands for Secure RTP, is an application layer security protocol.

V. DEFICIENCY OF SIP SECURITY MECHANISMS

Theoretically the SIP security mechanism through the SIP system can guarantee the confidentiality, integrity. Generally, SIP security mechanisms are difficult to deploy; and SIP security mechanism does not take into account the availability of the system and user privacy. For this reason some attack may happened.

A. Certification Attack

SIP authentication system has characteristics [6]: SIP system, the physical location of terminals are mobile, and therefore can not be the physical location information for certification, the basis of certification it required the authentication mechanisms. Required the use of password authentication password stored on the terminal, because every time, if users to enter a password, than this is unacceptable. VoIP terminals are complex systems, such as PC, therefore, the protection of such terminals are password on VoIP certification a key. Call for the global scope, different key system of systems required to exchange certificates, so VoIP systems need to increase management certification mechanism. Username, password helps to set the method. For example, it is not sure that the system or strategy to ensure the safety systems from malicious attacks Ways invasion; user name and Password Ways binding only at UA client interaction, but it does not protect the terminal interaction in the process of proxy servers and redirect the server's security.

B. DoS Attack

SIP security mechanism should not provide any protection for denial of service attack (DoS) , even if the use of TLS or IPSec can not protect the system from

DoS attacks. Because SIP server must be open to the public, so its become easily a denial of service attack. HTTP server vulnerable to distributed denial of service attacks, SIP servers can easily become a distributed denial of service attack. In addition, SIP UA on the denial of service attack protection is also limited, when denial of service attack occurs, SIP UA must be provide the alarm call support.

C. Spam attack

SIP protocol does not explicitly given to prevent Spam attack methods and mechanisms. e-mail system in an effective way to prevent Spam, such as: white list, black list, as well as content filtering and so on, are not suitable for SIP systems. SIP authentication mechanisms can not solve the Spam problem, because only SIP authentication mechanism to verify the user's identity, and should not validate the user's credibility, but also unable to verify whether the user is the initiator of Spam. For more effective anti-VoIP Spam, SIP authentication mechanism requires a combination of a number of strategies to prevent Spam in order to achieve better results.

VI. CONCLUSIONS

SIP is expected to be the future VoIP protocol of choice. SIP, as with other VoIP protocols, can be difficult to secure. SIP is an evolving protocol, which does not have security built in. SIP is vulnerable to attacks common to VoIP, as well as attacks unique to SIP. Your SIP system can be best secured by following best practices for securing VoIP and using standards-based security on all system components. These same security standards should be used as SIP is exchanged with components in an untrusted network. Use better SIP-security mechanism to prevent VoIP network from different attacks. SIP protocol provide the best possible protection where system-wide standards-based security is not possible.

REFERENCES

[1] Jeffrey Albers, Bradley Hahn, Shawn McGann, et al: An Analysis of Security Threats and Tools in SIP-Based VoIP Systems [EB/OL] September,2005
[2] Text Available at: www.colorado.edu/policylab/Papers/ Univ_Colorado_VoIIP_Vulner.pdf.
[3] Rosenberg J, Schulzrinne H, Camarillo G et al. SIP: session initiation protocol [EB/OL]. June 2002.
[4] Text Available at: http://www.ietf.org/rfc/rfc3261.txt.
[5] Si DF, Long Q, Han XH and Zou W, "Security mechanisms for SIP-based multimedia communication infrastructure," IEEE Conf. on Comm, Circuits and Systems (ICCCAS), ed. Proc. of 2nd ed., IEEE CS Press, 27-29 June 2004, pp.575-578.
[6] E. Nahum et al., "Evaluating SIP Proxy Server Performance," in Proc. NOSSDAV '07, 2007.
[7] Y. Rebahi, D. Sisalem: SIP Service Providers and the Spam Problem [EB/OL] April 2005
[8] Text Available at: http://www.snocer.org/Paper/.
[9] Joachim Posegga, Jan Seedorf: Voice Over IP:Unsafe at any Bandwidth [EB/OL]. April 2005.
[10] Text Available at: http://www.informatik.unihamburg.de /SVS/papers/ Eurescom_VoIP-unsafe.pdf.
[11] Mark Collier, "Basic Vulnerability Issues for SIP Security," SecureLogix Corporation, March 2005.