# SIP NETWORK SECURITY: ATTACKS, SECURITY MEASURES & MANAGEMENT

Shewaramani Jitendrakumar G.[1], Shah Tushar A.[2]
[1,2]Department of Computer Engineering,
BBIT, Vallabh Vidyanagar,
Gujarat, India
[1]shewaramani_jitendrakumar@gtu.edu.in
[2]bbit.tushar@gmail.com

**Abstract: In the research area of network security, secure communication in session initiation protocol is a major issue. In this paper we intend to discuss SIP protocol, network attacks on it, network security measures and solutions for SIP management. First we will introduce the SIP protocols in short and later we will draw focus on attacks, security measures and solutions**.

***Keywords:*** **SIP protocol network and its security**

## I. INTRODUCTION

Session Initiation Protocol (SIP) is a standard request-response protocol dealing with requests from clients and responses from servers typically used for telephony, instant messaging and Internet conferencing. SIP works in the Application layer of the Open Systems Interconnection (OSI) model. SIP can establish multimedia communication sessions or Internet telephony (VoIP) calls, and modifies, or terminates them. Because the SIP supports name mapping and redirection services, it makes it possible for users to initiate and receive communications and services from any location, and for networks to identify the users where ever they are.

## II. SIP BASED NETWORK ATTACKS: IDENTIFICATION

In today's Internet, nothing can be trusted, as intrusion, frauds and denial of service attacks have become out of control. Internet has become risky place for business losing lot of money in frauds.

To overcome the potential threats within SIP implementation, the IETF Engineering Task Force (IETF) is actively adding new procedures and enhancements to the protocol to further harden the protocol against network attacks. Hackers approach attacks in stages, beginning with probing of the network. Networks with open gateways and platforms with default passwords are looked for vulnerabilities by scanning. Once vulnerability is identified, it is used for larger attack. This is how hacker reaches different networks, traverse through all of these networks unnoticed, and launch large-scale DoS attacks on unsuspecting networks.

Below are some methods used when attacking a SIP based network.

**Registration Hijacking**: SIP uses clear text, so if a hacker captures these messages, then hacker can read subscribers' sensitive information such as their public and private identities. The hacker can use this information to gain access into the operator's network. Suppose a subscriber has registered with the network, and the subscriber's location is recorded by the registrar. All calls and e-mails, instant messages, and any other session traffic are sent to this location. Now hacker with the hacked information can access the same network and manipulate. To the network it appears as if the valid subscriber has changed locations in the network and sent a new registration since the hacker is using the identity of the valid subscriber. Hacker can now change his own registration with a new location that now gets stored in the registrar. This means that hacker can gain network access anytime he and also all session traffic for the valid subscriber will now be sent to the hacker's destination instead of the actual subscriber‘s device.

**Session Hijacking**: A Session Hijacking is used to take over a session in progress. Session hijacking began with the World Wide Web. If a web page is to keep active for longer time without providing authentication again and again web developers came with the concept of cookie: data file, usually consisting of the session ID. The Web server sends the browser the cookie when the site is first accessed. The cookie is then sent by the browser application each time it accesses the Web server for another page to identify itself. If these cookies are intercepted and copied, they allow the interceptor full access to the session already in progress. Cookies are somewhat controversial mostly because many believe they are executable rather than data files. The usage of cookies is full of vulnerabilities and making them very susceptible to session hijacking, so their use within a SIP network is not recommended.

**Impersonating a Server**: Many Web sites look exactly similar to their official sites but they are in fact hacker sites used for stealing information from unsuspecting consumers. Hackers create Web sites of that of a bank or credit card, using official logos which look exact like the real Web site. When the subscriber types in the URL for these sites, they get

redirected by a redirect server. The redirect server is compromised by the hacker to send consumers to their Web site rather than the real Web site. Sometimes the hacker send out e-mails with their links prompting consumers to go to the hacker's Web site to update their accounts or to claim refunds. Once the consumer has reached this site, they are asked for password information and other sensitive account information. This information is then stored on the server by the hacker and are misused. Here, of course possibility of compromising the DNS is also there. This is known as DNS poisoning, where the DNS server is hacked and the IP address for specific servers is changed to a spoofed Web site or address. This is very likely in SIP networks where DNS is used to identify the IP address for domains and their applications.

**Tampering with Message Bodies**: SIP is transferred in simple clear text, no decoder is needed. Capturing the message is enough which is not a hard task. After capturing a message, hacker can modify message body and headers of the SIP message. One of the solutions is Encryption of the text. Encryption prevents the hacker from being able to decipher the text, and therefore the hacker would be unable to change it and route it back to the network.

**DoS (Denial of service) and Amplification**: Denial of service (DoS) attacks can be launched using many different techniques. The easiest is simply flooding the network with specific traffic types. For example, using a call generator, a hacker can send millions of INVITEs into the network attempting to flood the network with call requests. We see these types of attacks take place many times, and they have even occurred in the PSTN. The use of SIP and IP provides much easier access to hackers, enabling these types of attacks much more frequently. Another form of DoS attack involves application servers. By launching a flood of requests to an application server, the network element is immediately flooded and congested, taking it out of service. This can also happen with the DNS through flooding with DNS queries. When the DNS is attacked, the entire network can be impacted, depending on where the server sits within the DNS hierarchy and whether or not redundancy has been implemented. Main goal of DoS is congestion, neither one request is enough nor is one target sufficient for such an attack. Therefore the attacker will use many targets and millions of requests, and will continue to send these requests until the congestion occurs. The registrar can also be the target of such an attack. A hacker can register a subscriber listing many different user identities for the same subscription. This then provides the registrar with a list of multiple destinations for a request. The hacker then launches requests toward the public identity, which the registrar and proxies then send to multiple destinations based on the registration made by the hacker. This is considered amplification, as the registrar is "amplifying" the effects of the attack by sending to multiple destinations. A similar kind of attack toward the registrar involves registering many different identities. Each identity consumes memory within the registrar, and therefore if a large number of registrations take place, the registrar runs out of memory. This only works in open networks with little to no security where anyone can register and use the services of the network to route requests. Hopefully most networks will prevent this from happening just through simple authentication, preventing unauthorized subscribers from accessing the registrar. At any rate, the end result is that the network becomes too congested to handle any further traffic and begins denying service to other subscribers. Some of the network elements may even crash due to the levels of traffic.

## III. SIP NETWORK SECURITY MEASURES

In Packet communication, security is the biggest concern. Security implementation can either be very robust and sophisticated or can be very simple. There are two types of attackers: one looking for easiest network to breach and other who take challenge of breaching very high security as they believe higher security means more confidential information and would be worth stealing.
There are basically six aspects to securing a SIP network:
Authentication: Authentication requires the use of passwords and the exchange of credentials. Whenever a subscriber registers location with the network, the registrar should always challenge the initial registration. Unfortunately, many networks do not challenge registrations. Instead they verify the user identity and trust that the identity is true. This is one of the reasons there are so many attacks on SIP networks today. Simply challenging the registrations could eliminate many security breaches.

**Authorization:** Authorization requires querying a database containing the basic account information for a subscriber. This account information provides the public as well as private identities for the subscription, and all the services the subscriber is authorized to access. This can be part of the authentication process to be most effective.

**Confidentiality:** Confidentiality protects the subscriber and the subscriber's identity. It ensures that conversations cannot be snooped on, and that the subscriber can exchange information freely without the information being captured by someone else. This remains one of the big challenges for network operators, especially given the many tactics being used today to capture sensitive data from subscribers.

**Integrity:** At the same time, it is equally important that the integrity of any data sent by a subscriber be sent intact without alteration. This includes any Web sites that may have been accessed as well. It is far too easy for hackers to access SIP messages and change the contents in an effort to change the service and where it is being delivered. It is also very easy to capture a SIP message containing text and alter the text message before it is delivered to its final destination.

**Privacy:** Privacy can sometimes be an issue when it is openly provided to anyone. Today on the Internet there are anonymous services where e-mails and other messages can be directed in an effort to hide the address of the originator,

and make it appear that the message came from someplace else. At the same time, privacy can also be offered as a feature to some clients who have a need for such a feature. For example law enforcement agents today when they make a call, the call does not give away their identity or the number they are calling from. This is an important service for them, and it should be maintained even in the SIP domain.

**Non-repudiation:** And finally, non-repudiation prevents subscribers from accessing services and later denying they used those services. If the operator implements the right tools and audit systems, you should have total visibility to every network transaction that takes place.

## IV. SECURITY SOLUTINONS FOR SIP MANAGEMENT

There are many reasons why many networks do not implement any form of security. Many platforms are older systems running operating systems that do not support security patches and must be completely replaced by newer platforms. This of course is cost prohibitive.
Other operators are severely short-handed and lack both the resources and the expertise to implement a strong security policy. They also lack the capital to invest in security implementations. Human error and configuration mistakes add to the problem, especially when expertise is lacking.
There are many different types of solutions available for securing networks. The security industry is probably one of the fastest growing tech sector's today with many different products available.
Let us now see various solutions available to protect a network from attack. These are not exclusive; there are numerous different solutions and approaches, but these should be considered as a bare minimum.

**Layering**: When looking at the various types of attacks, they are detected at different layers. Some detected at the lower layers, while others can only be detected at the application layers. One worthy change within security is the concepts of Layering of security implementations. Layering means implementing a security solution at all layers of the network. The concept of layering your implementations allows you to make the right amount of investment at each layer, without having to purchase very expensive solutions at one layer that does all. It also provides a much more robust platform, allowing you to provide various layers of security for different segments of the network and various applications and services.

**Intrusion Detection System**: Monitoring system was previously used which now has advanced and there is additional value as Intrusion Detection System (IDS). An IDS can operate in both real time as well as historical mode. A real-time system is needed for detecting attacks while they are in progress. However, these systems should also have some capacity of storage to allow for the investigation of network events at a later time. The amount of storage depends on the amount of traffic to be stored, and the duration of time you need to review. The IDS identifies the source of data (the network, application, or host). It performs analysis on the traffic based on rules (policy) and could also have the ability to establish its own policy through neural technology. The IDS then sends notification of the event to a console or other reporting system.
For example, in a flooding case, the monitoring system should detect an increase in the number of SIP requests across the entire network, as well as specific network segments. If the system also supports the configuration of thresholds, then the system can be set to alert the users anytime these thresholds are exceeded. This is important for identifying DoS attacks.
Another advantage to monitoring systems is the ability to measure the performance and set thresholds for the entire network, or critical network segments. Because the monitoring system has visibility to all network elements, and all network facilities, the system can therefore see traffic levels across the entire network rather than within just one entity. This could indicate (if it is a sharp rise in the number of requests) that there is a DoS attack underway.
An IDS performs analysis on previously collected data to determine if there is an attack underway, or abnormal events within the network. There are two types of methods that are used: signature analysis and anomaly analysis.
Signature analysis relies on rules that are defined within the IDS (also referred to as policy). These signatures are established from previous attacks, so they are signatures of known attacks used as profiles for detecting the same attacks again. These are very accurate, since they are based on known attack signatures. They are good for networks where expertise may not be abundant or resources are limited, but they should not be the only analysis used. Signature analysis is based on known attacks and therefore is not well suited for finding new attacks that use a different signature.
Anomaly analysis looks for abnormal behavior in the network. This is the best method for finding new attack signatures, but it does require additional expertise, since the analysis is usually a manual process today. Profiles are built based on a snapshot of captured traffic over a period of time. The longer the duration of time used to collect the traffic, the better the profile. One method may include setting thresholds in the network, and anytime these thresholds are exceeded, raising an alarm. Anything that deviates from the profile is then considered an anomaly.
These both methods should be used together for the most effective approach. A signature analysis implementation alone will not be effective in finding new attacks and will leave the network very vulnerable, since attack methods change regularly.

**Intrusion Protection System**: An intrusion protection system (IPS) combines the analysis of an IDS with the added protection of a firewall. The IPS then must be configured with a network address, since it will be an active element within the network. It is able not only to alter received traffic but to generate traffic. The IPS is capable of inspecting packets and altering packets, making them benign in the network. This allows rogue packets to continue in the network without

sending failure responses back to the originators, alerting them that their attempt was not successful.

The IPS can be implemented as part of the IDS, or it can be implemented separately. In this type of implementation the IPS could receive instructions or data from the IDS or from a policy engine.

The IPS can also be integrated on a host with an application. Vendors are continually adding security features within their platforms to further enhance their applications. This adds another level of security, but at a slightly higher cost, since it must be implemented at all critical applications.

An IPS, like an IDS, must support the network protocols used within the network. This includes any vendor-proprietary protocols that are implemented on vendor platforms. It makes decisions based on policy, although in some cases intelligence can be added that allows the IPS to operate in a neural fashion, creating new profiles and policy based on historical traffic patterns. This requires storing traffic from many months for the most complete profile. Many systems begin as passive IDSs and then later evolve into active IPSs. This is done by converting the passive probes to include active interfaces so that only those interfaces that are to be active would require a network address. This way, the passive capability can be maintained along with the active capability.

## V. CONCLUSION

The SIP protocol has become very popular protocol due to its simplicity and it being open protocol has gained acceptance by many communication equipment manufacturers. The current development of SIP-based devices and software clearly states that SIP will be the major technology providing all communication, including; video and audio conferencing, presence notification. But security issues rising due to simplicity of the protocol will also have to be taken care of and accordingly necessary methods have to been implemented.

## REFERENCES:

[1] A. Mankin, S. Bradner, R. Mahy, J. Ott, B. Rosen *Change Process for the Session Initiation Protocol*, RFC 3427, December 2002

[2] Handley, H., Schulzrinne, H., Schooler, E. and J. Rosenberg, *SIP: Session Initiation Protocol*, RFC 2543, March 1999.

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, June 2002.

[4] *Microsoft Real-Time Communications: Protocols and Technologies*, Conference on Computer Vision and Pattern Recognition.

[4] A Shashua "-Geometry and Photometry in D Visual Recognition". PhD The Sis. MIT Cambridge.

[5] DJ Beymer "Face Recognition Under Varying Pose Technical Report" MIT Artificial Intelligence Laboratory.

[6] AS Georghiades , P N Belhumeur and D J Kriegman "Illumination Based Image Synthesis" Creating Novel Images of Human Faces Under Differing Pose and Lighting " In Proc Workshop on Multi View Modeling and Analysis of Visual Scenes.

[7] T Vetter and T Poggio "Linear Object Classes and Image Synthesis From a single Example Image" IEEE vol 19.

[8] L.Wiskott, J M Fellous, and C vonder Malsburg, "Face Recognition by Elastic Bunch Graph Matching", IEEE Tran's vol 19.

[9] A Pentland, B Moghaddam, T Starner,Viewbased and Modular "Eigenspaces for Face Recognition" in Proc. Conference on Computer Vision and Pattern Recognition.

[10] D J Beymer and T Poggio "Face Recognition from One Example" View in Proceedings International Conference on Computer Vision.