Chapter 3
Security Analysis and Literature Survey

SIP adopts either basic or HTTP digest authentication for authenticating SIP Client (UA) to SIP servers (US) [30]. Strong authentication is needed to prevent against several kinds of attacks, such as registration hijacking, call hijacking, replay attack and Man-in-the-Middle attack impersonation.

3.1 Analysis of Security in SIP

In the following section we have analyzed the SIP protocol and its authentication scheme, which helps us to find out vulnerability in it and motivation of our research work.

- All SIP messages is exchange in clear text format, result of this is attacker can easily intercept and reuse the credential of major signaling message.
- HTTP Digest authentication protects user credential by using a cryptographic hash function (MD5), which is vulnerable to message digest attack.
- HTTP Digest authentication scheme supports one-way authentication of SIP message.
- According to RFC 3261, HTTP Digest authentication scheme does not support message integrity and confidentiality of the SIP messages [11]. Additionally, some SIP messages (e.g. BYE, CANCLE, ACKs) authentication is based on the credentials generated by previous requests. This implies that a malicious user may send a manipulated message to cause DoS.
- HTTP Digest authentication requires a pre-arranged trusted environment for password distribution and passwords may be stored either in plaintext or cipher text form in the server side. 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. Besides that, the absence of any correlation between the user name and the SIP URIs gives the opportunity to a malicious user to masquerade as a legitimate user.
- SIP does not support strong authorization model, it is possible for an attacker to gain access to services that are normally offered to legitimate users. A SIP security specific header (Proxy-Authenticate, Proxy-Authorization, and WWW Authentication) does not carry enough information to authorized UA to access certain services of server.
- Proxy Server or Registration server only check authenticity of the INVITE and REGISTER SIP messages and leaves other SIP messages (e.g., TRYING, RINGING, 200 OK, ACK and BUSY)
unprotected[22]. While SIP authentication process encodes URL, username and realm but leaves other fields (e.g., SDP, From, To) in unprotected format [22].

- Attacker can terminate an established VoIP session by sending BYE message to UA. UA will not check whether BYE massage has come from authorized source or unauthorized source.

As discussed earlier HTTP Digest authentication is not sufficient to prevent eavesdropper and Man-in-the-Middle (MITM) to intercept and break credential information. Result of this is VoIP system is vulnerable to replay and MITM attack, MITM can prolong the duration of call established between two VoIP subscribers. During presence of MITM, VoIP system is susceptible to billing threats such as Invite Replay, Fake Busy, Bye Delay and Bye Drop attacks. In addition to this above discussed SIP flaws make VoIP system vulnerable to various severe threats such as Force teardown attack Denial Of Service attacks (DoS) like Invite Flooding, Cancel and Bye attack.

### 3.2 Related Work on VoIP Threats

Due to the text based nature of SIP protocol, all SIP messages will exchange in clear text format between communicating party, in addition to this SIP supports basic/HTTP based digest authentication which is not sufficient to protect SIP message. Result of this is SIP based VoIP system is vulnerable to confidentiality, integrity and availability threats. In next section, we have discussed related work to address confidentiality threats, eavesdropping, interception and modification threats, integrity threats, Man-in-the-Middle and DoS attack.

#### 3.2.1 Confidentiality Threats

Confidentiality threats are serious issues in VoIP system compared to the traditional PSTN. Confidentiality refers to the protection of data from being read by an unauthorized user. Historically, an attacker would need physical access in order to eavesdrop on a conversation or illegitimately access the telephone service. Since VoIP uses open protocols and public networks, a number of attack vectors exist which the proprietary nature of the PSTN had previously protected access to the media and signaling.

#### 3.2.2 IP Spoofing

VoIP system is based on Internet Protocol (IP). The most prevalent vulnerability in IP is address spoofing. In a VoIP environment, an attacker can impersonate many different devices by spoofing those devices IP addresses. These devices include: registration servers, SIP proxy servers, IP phones, Media Gateway Control Protocol (MGCP) servers, and Domain Name Server (DNS). By
impersonating a valid user of IP phone through spoofing, an attack can use the VoIP system to make unauthorized calls.

Patrik Park [32] has discussed about the valid or invalid call request flooding: Most VoIP servers have a security feature that blocks flooded call requests from unregistered endpoints. So, an attacker registers first after spoofing a legitimate user and then sends flooded call requests in a short period of time (for example, 10,000 SIP INVITE messages per second). This impacts the performance or functionality of the server regardless of whether the request message is valid or not.

Luo et al. [23] experimentally evaluate the susceptibility of SIP to CPU-based denial of service attacks. They use an open-source SIP server in four attack scenarios: basic request flooding, spoofed-nonce flooding (wherein the target server is forced to validate the authenticator in a received message), adaptive-nonce flooding (where the nonce is refreshed periodically by obtaining a new one from the server), and adaptive nonce flooding with IP spoofing. Luo has also discussed that these attack have large impact on QoS provided by the servers. They propose several countermeasures against such attacks, indicating that authentication by itself cannot solve the problem and that, in some circumstances, it can exacerbate its severity. These mitigation mechanisms include lightweight authentication and white listing, proper choice of authentication parameters and binding nonce to client IP addresses.

3.2.3 Eavesdropping, Interception and Modification threats

These threats cover situations where an adversary can unlawfully and without authorization from the parties concerned listen in on the signaling (call setup) or the content of a VoIP session, and possibly modify aspects of that session while avoiding detection.

Jeffrey Albers et al. [24] found out new approach of eavesdropping. They have discussed that knowing the IP address of a phone can allow an attacker to specifically target that phone for eavesdropping or spoofing. One method for eavesdropping on conversations involves spoofing the default gateway’s IP address on a phone to redirect all VoIP packets to an attacker’s machine. With traditional IP forwarding this kind of attack can remain hidden from intrusion detection systems. IP phones with remote administration capabilities severely increase the risk of this type of attack. Implementing network layer filtering through the use of a firewall can reduce the risk of this kind of attack.

Takahashi and Lee [25] examine the problem of covert channels in VoIP protocols, identifying and quantifying several ways in which data can be surreptitiously leaked out of a user’s system or an enterprise network. As an example, they demonstrate the steganographic insertion of a second
voice channel in a SIP-based VoIP conversation. They have proposed a technique which has the potential of leaking a secure (encrypted) conversation through a secondary channel, or can be used to hide the true communication content from an eavesdropper.

3.2.4 Integrity Threats

An unauthorized user may perform unauthorized operations like delirious modification, destruction, deletion or disclosure of switch software, data and message between two UA.

The basic method of the integrity threat is altering messages (signals) or media after intercepting them in the middle of the network. That is, an attacker can see the entire signaling and media stream between endpoints as an intermediary. The alteration can consist of deleting, injecting, or replacing certain information in the VoIP message or media.

Patrick Park [26] has discussed the two types of integrity threats.

- Threats against message integrity (message alteration)
- Threats against media integrity (media alteration)

**Message alteration** is the threat that an attacker intercepts messages in the middle of communication entities and alters certain information to reroute the call, change information, interrupt the service and so on. The typical examples are called rerouting and black holing.

**Media alteration** is the threat that an attacker intercepts media in the middle of communication entities and alters media information to inject unauthorized media, degrade the QoS, delete certain information, and so on. The media can be voice-only or integrated with video, text, fax, or an image.

Mark collier [27] has discussed registration hijacking which is result of weak authentication between User Agent (UA)/IP phone and SIP proxy/registrar (or IP PBX). Registration hijacking occurs when an attacker impersonates a valid UA to a registrar and replaces the legitimate registration with its own address. He has suggested the mitigation technique by using TLS.

Liancheng Shan et al. [28] exposed another type of Registration Hijacking attack where attacker disguised as legitimate UA register and replaces the legitimate user's registered address. This attack led to the legitimate users of all incoming calls to be sent to the attacker on registration of UA.

3.2.5 Man-in-the-Middle (MITM) Attack

Wang et al. [29] evaluated the resilience of three commercial VoIP services (AT&T, Vonage and Gizmo) against Man-in-the-Middle adversaries. They show that it is possible for an attacker to divert and redirect calls by modifying the RTP endpoint information included in the SDP exchange.
(which is not protected by the SIP Digest Authentication) and to manipulate a user’s call forwarding settings in the latter two systems. These vulnerabilities permit for large-scale voice pharming, where unsuspecting users are directed to fake interactive voice response systems or human representatives. The authors argue for the need for TLS or IPSec protection of the signaling.

Zhang et al. [30] show that by exploiting DNS and VoIP implementation vulnerabilities, it is possible for attackers to perform Man-in-the-Middle attacks even when they are not on the direct communication path of the parties involved. They demonstrate their attack against Vonage, requiring that the attacker only knows the phone number and the IP address of the target phone. Such attacks can be used to eavesdrop and hijack the victims’ VoIP calls. The authors recommend that users and operators use signaling and media protection, conduct fuzzing and testing of VoIP implementations, and develop a lightweight VoIP intrusion detection system to be deployed on the VoIP phone.

Zhe Chen et al. [31] has discussed the principle of the MITM-DoS attack is to insert “especial” sip messages forged by the MITM, interrupt the communication between the UAs or the UA and Server and launch the DoS attack to either the UAs or the Server. He has discuss various approach of MITM, in the first approach MITM will held between two communicating party (UAs). Once the UA knows the other UA’s IP, they can communicate with each other directly. The IP can be attained by the SIP redirect server or by the previous communication. It is possible to launch the MITM attack because of the unilateral authentication between the UA and Server in the SIP VoIP system. So the MITM can easily inject the communication into them, trick the UAs into communicating with him rather than with each other. The MITM will not only see all signaling being exchanged, but can also change information being transmitted. After session initiation MITM will send BYE to both UA and terminate the session.

In second approach, attacker acts himself as the caller and sends CANCEL message to the callee before sending the final response to the caller. When the callee receives the CANCEL message, he thinks that the caller doesn’t want to communicate with him and hangs up the telephone. Immediately the caller hears the busy tone. That is to say the callee refuses to provide the voice service and the MITM-DoS attack to the callee is successful.

In third approach of MITM exists between communicating party and cause MITM DoS attack by sending SIP respond messages. MITM sends forge 486 message (486 Busy Here) after 180 Ringing message. After INVITE message MITM cause DoS attack by sending error response code 1xx, 2xx, 5xx, 6xx to Callee.
Bremler-Barr et al. [32] describes de-registration attacks in SIP, wherein an adversary can force a user to be disassociated with the proxy server and registrar, or to even divert that user’s calls to any party (including to the attacker). This attack works even when authentication is used, if the adversary can eavesdrop on traffic between the client and the SIP proxy. They demonstrate the attack against several SIP implementations, and propose a protection mechanism one way hash function motivated by the onetime password mechanism.

3.2.6 DoS Attack

Zhang et al. [33] describes a denial of service attack wherein adversaries flood SIP servers with calls involving URIs with DNS names that do not exist. Servers attempting to resolve them will then have to wait until the request times out (either locally or at their DNS server), before they can continue processing the same or another call. This attack works against servers that perform synchronous DNS resolution and only maintain a limited number of execution threads. They experimentally show that as few as 1,000 messages per second can cause a well provisioned synchronous-resolution server to exhibit very high call drops, while simple, single-threaded servers can be starved with even 1 message per second. As a countermeasure, they propose the use of non-blocking DNS caches, which they prototype and evaluate.

Reynolds and Ghosal [34] describe a multi-layer protection scheme against flood based application and transport-layer denial of service (DoS) attacks in VoIP. They use a combination of sensors located across the enterprise network, continuously estimating the deviation from the long-term average of the number of call setup requests and successfully completed handshakes. Similar techniques have been used in detecting TCP SYN flood attacks, with good results. The authors evaluate their scheme via simulation.

Ormazabal et al. [35] describes the design and implementation of a SIP-aware, rule based application-layer firewall that can handle denial of service (and other) attacks in the signaling and media protocols. They use hardware acceleration for the rule matching component, allowing them to achieving filtering rates on the order of hundreds of transactions per second. The SIP-specific rules, combined with state validation of the endpoints, allow the firewall to open precisely the ports needed for only the local and remote addresses involved in a specific session, by decomposing and analyzing the content and meaning of SIP signaling message headers. They experimentally evaluate and validate the behavior of their prototype with a distributed test bed involving synthetic benign and attack traffic generation.
Hyun-Soo et al. [36] proposes a detection mechanism for de-registration and other call disruption attacks in SIP that is based on message retransmission: when a server receives an unauthenticated (but possibly legitimate) message M that could disturb a call or otherwise deny service to a user, it asks the user's agent to retransmit the last SIP message sent by that agent, as an implicit authenticator. If the retransmission matches M (i.e., this was a legitimate request), the server proceeds with its processing. If the retransmission does not match M, or if multiple retransmissions are received within a short time window (as may be the case when an attacker can eavesdrop on the network link between the SIP proxy and the user, identifying the request for retransmission), M is discarded. However, the scheme requires a new SIP message to signal that a retransmission is needed. Geneiatakis and Lambrinoudakis [36][37] consider some of the same attacks and propose mitigation through an additional SIP header that must be included in all messages and can cryptographically validate the authenticity and integrity of control messages.

Sengar et al. [38] describe vFDS, an anomaly detection system that seeks to identify flooding denial of service attacks in VoIP. The approach taken is to measure abnormal variations in the relationship between related packet streams using the Hellinger distance, a measure of the deviation between two probability measures. Using synthetic attacks, they show that vFDS can detect flooding attacks that use SYN, SIP, or RTP packets within approximately 1 second of the commencement of an attack, with small impact on call setup latency and voice quality.

R. Shanmugavadivu et al.[39] has developed an anomaly based intrusion detection system in detecting the intrusion behavior within a network. A fuzzy decision-making module was designed to build the system more accurate for attack detection, using the fuzzy inference approach. An effective set of fuzzy rules for inference approach were identified automatically by making use of the fuzzy rule learning strategy, which are more effective for detecting intrusion in a computer network.

Iftikhar Ahmad et al.[40] adopts a supervised neural network phenomenon that is majorly used for detecting security attacks. The proposed system takes into account Multiple Layered Perceptron (MLP) architecture and resilient back propagation for its training and testing. The system uses sampled data from Kddcup99 dataset, an attack database that is a standard for evaluating the security detection mechanisms. But proposed IDS fail to generate low error rate and high detection ration. System can not specify severity of attack so that user can take appropriate precautionary measure to protect VoIP system.

Niccolini et al. [41] designed intrusion detection/intrusion prevention system architecture for SIP based VoIP system. Proposed system uses both knowledge-based and behavior-based.
detection, arranged as a series in that order. They develop a prototype implementation using the open-source Snort IDS. Niccolini has evaluate the effectiveness of system in an attack scenario by measuring the mean end-to-end delay of legitimate SIP traffic in the presence of increasing volumes of malformed SIP INVITE messages.

Wu et al. [42] designed an intrusion detection system, called SCIDIVE that is specific to VoIP environments. SCIDIVE aims to detect different classes of intrusions, can operate with different viewpoints (on clients, proxies, or servers), and takes into consideration both signaling (i.e., SIP) and media-transfer protocols (e.g., RTP). SCIDIVE’s ability to correlate cross-protocol behavior, theoretically allows for detection of more complex attacks. However, the system is rule-based, which limits its effectiveness against new/unknown attacks.

Bertrand et al. [43] proposed an anomaly detection technique for identifying and blocking SPIT that creates caller profiles based on their IP address. The criteria used by in their analysis includes number of received error messages, the use of a directory service, whether multiple calls are placed by the same caller, the duration of calls and the variance of call duration across multiple calls, and the number of simultaneous incoming calls (from multiple different users) to the same user.

In next section we have analysis and conclude above discussed literature survey.
3.3 Analysis of Survey

During literature survey, we have identified various VoIP threats which we have classified by their type in four major categories e.g. integrity, confidentiality, availability and finally social threats. Threats taxonomy consists VoIP, SIP threats. Figure 3.1 shows VoIP taxonomy. [5] [70] [26].

**Figure 3.1** Taxonomy of threats on VoIP System
We have observed that authors have attempted to address VoIP vulnerability by proposing new solution or implementing existing secured protocol such as S/MIME, IPSec. In addition to this, study of various IDS has inspired us to design new adaptive IDS to protect VoIP system from DoS attacks. During literature survey, we have observed that authors have discussed media related attacks and their protection.

In next section we have attempted to analyze and conclude literature survey based on security strength, weakness and feature of well known protocols, which motivates us to see these problems in different angle.

- SIP messages are capable of carrying MIME bodies, and the MIME standard includes mechanisms for securing MIME contents to ensure either integrity or confidentiality by means of the multipart/signed and application/pkcs7-mime MIME types [72]. S/MIME provides a set of functionalities and SIP utilizes two of them: Integrity and authentication tunneling and Tunneling Encryption. However, this solution mandates the deployment of a global S/MIME Public Key Infrastructure (PKI) but the largest outstanding defect with the S/MIME mechanism is the lack of a prevalent public key infrastructure. Alternate to PKI is exchanged public keys would be self-signed, which makes the initial key exchange susceptible to man-in-the-middle attacks.

- IPSec offers confidentiality, integrity, data-origin authentication services, as well as (optionally) anti replay and traffic analysis protection by utilizing the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols. In IPSec it is necessary to have pre-established trust among the communicating parties and it can only be utilized in a hop-by-hop fashion. Most of client does not implement IPSec client because IPSec is implemented at the operating system level, result of this it protect the traffic between the corresponding network servers. Moreover, SIP specifications do not suggest any framework for key administration, which is required by IPSec.

- Transport Layer Security (TLS) protocol supports [71] authentication, confidentiality of messages. TLS has many of the advantages of IPSec and the successful introduction of the protocol in the wired internet has proved its usability and effectiveness. Details comparisons of TLS and IPSec are given in Table 6.1. Likewise, TLS can be part of SIP environment, as it runs above TCP/IP and higher-level protocols such as HTTP or FTP, consequently the TCP header is not encrypted. However, TLS cannot be combined with UDP and it does not assume any trust relation among communicating parties.
It is worth noticing, that IPSec and S/MIME generate considerable overhead in SIP messages. More importantly they cannot protect the integrity and confidentiality of the entire SIP message due to existing restriction of header modification, as intermediate nodes must have access to SIP header to process and route the SIP message to the appropriate destination.

In some cases, security services may require the combination of TLS and S/MIME to provide the "end-to-middle security" to secure the information passed between the UA and intermediaries. End–to-middle security is use only in such model where trusted and partially-trusted proxy servers are mixed along a message path. In “end-to-middle security” model TLS uses to support integrity and authentication, while S/MIME is used to provide mainly privacy for some parts of the transmitted data. [73]

Salsano et al. [44] conduct an evaluation of the processing costs of SIP calls that involve authentication, under different transport, authentication and encryption scenarios. They show that a call using TLS and authentication is 2.56 times more expensive than the simplest possible SIP configuration (UDP, no security). However, a fully-protected a call takes only 54% longer to complete than a configuration that is more representative than the basic one but still offers no security; the same fully-protected call and has the same processing cost if the transport is TCP without any encryption (TLS). Of the overhead, approximately 70% is attributed to message parsing and 30% to cryptographic processing. With the advent of Datagram TLS (DTLS), it is possible that encryption and integrity for SIP can be had for all configurations (UDP or TCP) at no additional cost.

3.4 Conclusion

During the literature survey, it has been observed that author’s have attempted to mitigate SIP vulnerability using well known protocols such as S/MIME, IPSec and TLS. Table 3.1, shows the summary of well known protocols based on their security features.

<table>
<thead>
<tr>
<th>Security Feature</th>
<th>S/MIME</th>
<th>IPSec</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Authentication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support Integrity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support Confidentiality</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support hop-to-hop security</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support end-to-end security</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
After security analysis of S/MIME, IPSec and TLS protocols, we have observe that,

1. S/MIME supports integrity or confidentiality at end-to-end fashion but fails to support PKI and also adds considerable overhead on SIP protocol.
2. IPSec provide PKI based authentication, integrity and confidentiality on hop-to-hop basis but a pre-established trust is required between the communicating parties.
3. TLS support confidentiality, authentication, it works well with SIP protocol but does not work with connectionless transport protocol such as UDP.

In-depth of literature survey and analysis of these protocols based on security feature. We have concluded that presently TLS is better alternate option as compare to IPSec and S/MIME and TLS supports secured exchanging of signaling message between two communicating party.

We have also found little research (9.6%) is going towards addressing the problem of denial of service, DoS attacks are the result non availability of resources as well as organization revenue losses [74]. Some DoS prevention techniques are based on retransmission of message but it added extra network traffic. From above finding, it is essential to address these attacks to next level with fresh attempts. This thought has motivated us to design new IDS.