**Indonesian Journal of Electrical Engineering and Computer Science**
Vol. 7, No. 2, August 2017, pp. 457 ~ 465
DOI: 10.11591/ijeecs.v7.i2.pp457-465


# Survey of SIP Malformed Messages Detection

**Mourade Azrour*, Mohammed Ouanan, Yousef Farhaoui**
Moulay Ismail University, Faculty of sciences and Techniques,
Department of Computer Science, M2I Laboratory, ASIA Team, Errachidia, Morocco.
*Corresponding author, email: azrour.mourade@gmail.com

***Abstract***

*Session Initiation Protocol (SIP) is an application layer protocol designed to control and establish multimedia sessions over internet. SIP gaining more and more popularity as it is used by numerous applications such as telephony over IP (ToIP). SIP is a text based protocol built on the base of the HTTP and SMTP protocols. SIP suffers from certain security threats which need to be resolved in order to make it a more efficient signaling protocol. In this work, we review the proposed works aimed to detect SIP malformed messages that can cause security problem. Then, we classify the type of SIPmalformed message and compare between the mechanisms used to reinforce the detection of SIP malformed message attack.*

***Keywords****: Malformed message detection, Session Initiation protocol, Security; Attack*



## 1. Introduction

Nowadays, the growth of the internet has brought with it a numerous advantages and has changed the human life. Therefore, online services are coming more in the more important in humane activity. Telephony over IP (ToIP) is one of those services, it can defined as technology that uses the IP protocol to exchange flux multimedia (voice, text, video...), which are traditionally transferred over the Public Switched Telephone Network (PSTN). The voice and data are transferred in the form of packets over a Local Area Network (LAN), or over the Internet Area Network (IAN).

In recently years, the Session Initiation Protocol (SIP) is a most popular signaling protocol developed to set up, alter, and tear down multimedia sessions among deferent participations [1]. As SIP is a text based protocol and offers many advantages, it is a target of attackers. Therefore, SIP suffers from various attacks. In practically, malformed SIP message attack is one of the significant attacks, because it can be used to interrupt the system, to access to the privacy area, or to execute a malicious code.

Many researches have been made to deal with the problem [2-9], these research are based on deferent techniques to detect SIP malformed messages and to prevent the system. Other researches [10-15] are concentrated on the authentication of message SIP which is the required security service for SIP.

In this paper, we review the some known proposed works which are based on detection of SIP malformed messages. Then, we compare between the mechanisms used in order to reinforce the detection of SIP malformed message.

The rest of this paper is organized as following. The section 2 delivers the general information about SIP. In the section 3, we classify the type of SIP malformed messages. The comparison between the deferent proposed works is made in the section 4. In the last section our paper is concluded.

## 2. SIP Overview

### 2.1. SIP Architecture

The architecture of SIP consists of a proxy server, redirect server, registrar server, location server, and user agents. The Figure 1 illustrates the components of SIP architecture. The role of each component is described as follows:

*Received May 6, 2017; Revised July 5, 2017; Accepted July 19, 2017*

a. User Agent Client (UAC): generates SIP requests before they were sent.
b. User Agent Server (UAS): generates answers to SIP requests (accepting, refusing, or redirecting).
c. User Agent (UA): it can be a SoftPhone (software) or HardPhone (IP phone). It is able to generate, send and receive SIP requests. It can act at the same time as a UAC and UAS.
d. Registrar Server: handles the registration of SIP terminals. This is a server that accepts SIP REGISTER requests.
e. Proxy Server: it is a server which is connected to fixed or mobile terminals (UA). It plays the role of a server and client.
f. Redirect Server : it is a server that accepts SIP requests, translates the SIP address of a destination to IP address and returns them to the client.
g. Location server: It provides the proxy server, redirect server, and register server, it allows for them to look up or register the location of the user agent.

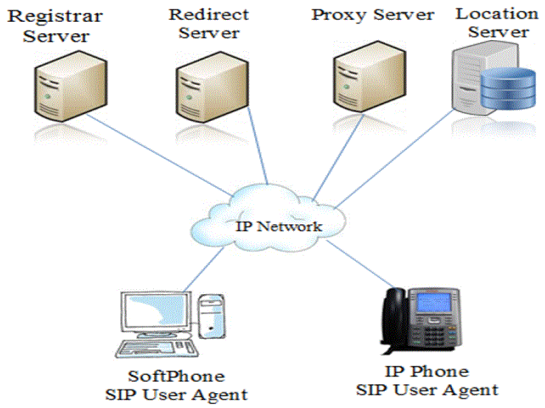


Figure 1. SIP Architecture

### 2.2. SIP Message

A SIP message is either a request from a client to a server, or a response from a server to a client. A SIP messages consist of a start-line, header fields, an empty line representing the end of the header fields, and a message-body which is optional.

SIP requests are caracterised by having a Request-Line for a first-line. A Request-Line contains a method name, a Request-URI, and the protocol version separated by a single space character. SIP defind six original methodes in RFC 3261 which are REGISTER for registering contact information, INVITE, ACK, and CANCEL for setting up sessions, BYE for terminating sessions, and OPTIONS for querying servers about their capabilities. The other methods SUBSCRIBE, REFER, MESSAGE, NOTIFY, UPDATE, INFO, and PRACK are descibed as optional in other RFC's. An example of SIP request message is shown in Figure 2.

SIP responses are distinguished from requests by having a Status-Line as their start-line. A Status-Line contains the protocol version, a numeric Status-Code, and its associated textual phrase, with each element separated by a single space character. As detailed in the Table 1 the first digit of the Status-Code defines the class of response. An example of SIP responses are illustrated in Figure 3.

```
REGISTER sip:192.169.1.2:5060 SIP/2.0
Via: SIP/2.0/UDP
192.168.1.2:16999;rport;branch=z9hG4bKPj82050b9f03844659a2
b24641722ca1a1
Route: <sip:192.169.1.2:5060;lr>
Max-Forwards: 70
From:
<sip:M.azrour@192.169.1.2>;tag=5c2fe1808e4a4fa9b0d6a6ecfd29
7e0b
To: <sip:M.azrour@192.169.1.2>
Call-ID: 5b3d61c6c6654bf0989d21b9e4c92300
CSeq: 63287 REGISTER
Allow: INFO, PRACK, SUBSCRIBE, NOTIFY, REFER, INVITE,
ACK, BYE, CANCEL, UPDATE
Contact: <sip:M.azrour@192.168.1.2:16999>
User-Agent: StarTrinity.SIP 2017-04-05 14.41 UTC
Expires: 3600
Content-Length: 0
```

Figure 2. Example of SIP request message

```
SIP/2.0 407 Proxy Authentication required
CSeq: 1 SUBSCRIBE
Call-ID: 239677225434@192.168.1.3
From: <sip:azrour@192.168.1.2>;tag=z9hG4bK18860624
To: <sip:azrour@192.168.1.2>
Via: SIP/2.0/UDP
192.168.1.3:46229;rport=46229;branch=z9hG4bK84193;received=
192.168.1.3
Proxy-Authenticate: Digest
realm="myrlm.net",nonce="4b7f9a75667b27d5b2365
9b8e0c0da79",opaque="",stale=FALSE,algorithm=M
D5
```

Figure 3. Example of SIP response message

Table 1. Message response code

| code | meaning | example |
|---|---|---|
| **1xx** | Provisional | 100 Trying<br>180 Ringing |
| **2xx** | Success | 200 OK<br>202 Accepted |
| **3xx** | Redirection | 300 Multiple Choices<br>301 Moved Permanently |
| **4xx** | Client Error | 401 Unauthorized<br>407 Proxy Authentication Required |
| **5xx** | Server Error | 500 Server Internal Error<br>502 Bad Gatew ay |
| **6xx** | Global Failure | 600 Busy Everywhere<br>603 Decline |

### 2.3. SIP Operation

The communication in SIP environment is based on request and response. As illustrated in Figure 4, to register its location in the server, the user has to send request REGESTER to the server. After receiving this request and if the authetication is requered, the server verify the existing of the Authorization header field, if not, the server send a response having a code 407 (proxy authentication required) back the user. Therfore the user resend the REGISTER request with the Authorization header. Upon receiving this request the server verify the existence of the Authorization header field and check the validity of the authetication parameters. If ok, the server send response having a code 200 ( OK) back to user.

## 3. SIP Malformed Messages

### 3.1. Types of SIP Malformed Messages

The malformed message is any type of invalid message, generally formed by an attacker to exploit and eventually take advantage of any implementation gap or dysfunction might exist in the target system [16]. In SIP environment malformed message is any SIP message which having the format that is incompatible with the norms defined in RFC 3261 [1].

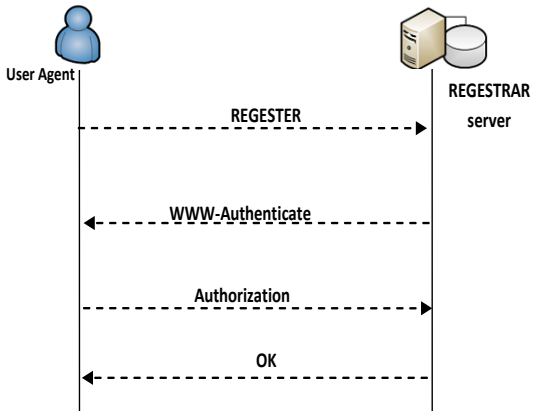


Figure 4. Example Registration Scenario

1. SQL Injection

SQL (structured query language) injection is type of SIP malformed message in which an attacker can execute SQL code by exploiting the Authorization header field [16]. In the original authetication protocol HTTP Digest [17], when user agent request to access to the server's service, the server send response having a code 407 (proxy authentication required), this response means that the user agent must firsty authenticate itself with the server before the request can be processed. To replay to this challenge, the user agent used the Authorization header field to carry its credentials in a new request. Upon received the user's request which contains the Authorization, the sever recomputes the user's credentials using the password stored in its database. So, the server requests its database to extract user's registred parameters.

As showed in Figure 5 the authorization field contains the credentials of azrour; the nonce was supplied by the SIP server located at the URI specified. The responses contain the hashed username and password. The value of opaque is empty.

```
Authorization:Digestusername="azrour",
realm="mydomain.com", algorithm="md5"
nonce="245a5b87ca911568ae34300023fa2",
opaque="", uri="sip:admin@mydomain.com",
response="96f848e6765b453b3434cc341e5f1"
```

Figure 5. Example of Authorization header field

Now, suppose that an attacker has send to the server a request message with authorization field but contains SQL code as shown in Figure 6. After receiving and executing the SQL injedted code the server will lose all stored user's information.

```
Authorization:Digest username="mourade",
Delete from nam_of_table
realm="192.168.1.122",
nonce="ac45a1658ae3439843423fa2",
opaque="",uri="sip:192.168.1.122",
response="34a848e6765b453b3b34dcc341e5f1"
```

Figure 6. Example of SIP malformed message with SQL code

2. Message with incorrect method in first Line

As discribed in the RFC 3261, SIP message is started by Fisrt-line. If the message is a request the Fisrt-line contains a method name, a Request-URI, and the protocol version separated by a single space character. If it is a response it contains the protocol version, a numeric Status-Code, and its associated textual phrase. If any message is send with ainvalid method or invalid Status-Code it will be considred as abnormal, even if the rest of the message is valid.

3. Message withinvalidsyntax

The syntax of SIP message is considered as invalid if one or more mandatory fields are not existe or if an unique field is duplicated. For example if the field "To" is not existed the message will never rechead its destination. In the other hand if this field is duplicated the intermediate servers will be disturbed and will not know the exate destination of the message.

4. Message with invalid values

In some time it happen that the syntax of the message is correct but, one or more values of the fields is not valid, or it is null, or contains a value that can causes undesirable result in the system. Therefore, these type messages must be considered as abnormal messages. For example if the Expires's value or the Date's value are negative (e.g. -8, April -2 2017) this value are invalid because the time and the date are always positive.

### 3.2. Objectives of SIP Malformed Message

Due to its using in the IP network, SIP inherits some vulnerabilities of TCP/IP protocol, in addition to its specific threats. SIP malformed message attack is one of the attack that targeting SIP component. This attack can be executed by a legitimate user that trying to send a malformed messages to discover the weakness of the system, or sending a malformed message by error. Nevertheless, an outsider attacker can try to have an unauthorized access to some private services, or attempt to crush the server. Generally, we can classify the objectives of the SIP malformed message into the following.

```
SIP_METHOD SIP-URI|SIPS-URI MESSAGE HEADER+
[MESSAGE_BODY]

Additional rules
SIP_METHOD !=NULL
MESSAGE_HEADER!=NULL
size_of(SIP_METHOD)>%constant%e.g. 50 bytes
size_of(MESSAGE_BODY)>%constant%
```

Figure 7. Geneiatakis et al.'s general detection signature for SIP

1. Discover and exploite the vulnerabilities of SIP server

The attacker can try to compose and send all possible malformed SIP message to discover the weakness of the server.

2. *Force SIP server to execute malicious code*

This objective can be obtained when an attacker has success to execute SQL code injected in Authorization field.

3. Unauthorized access

The sending of SIP malformed message with SQL code which adding or modifying the user parameters (username, password) in the server database, give the unauthorized access to the attacker.

4. Turne down SIP server

When SIP server try to process the received malformed message which contain invalid (e.g. invalid type of field) an exception can be detected, so if the programmer have not treat this exception (in source code) the server may be blocked and turn down.

## 4. SIP Malformed Message Detection

### 4.1. Analysis of Existing Solution

In order to protecte SIP against malformed message attacks, Geneiatakis et al. [2] have proposed the detection mechanism which can be descibed through a specific structrues named "attack signatures". The proposed mechanism consists on two parts based on the SIP syntax. The first part is used to identify the malformed message, and it can be applyed to any SIP methods. Hence, it known as general signature, an example of this signature is illustrated in Figure 7. The second part is optional because it includes additional rules specific for each SIP methodes. In the Figure 8 where the exemple of SIP INVITE message is dipected, we can show that the mondatory and unique fields are marked with "*" caracter. Therefore, if any one of these fields is not exist or is duplicated, the message will be considered as abnormal.

```
INVITE_METHOD SIP-URI | SIPS-URI MESSAGE HEADER+
MESSAGE HEADER=Via| Max-Forwords| From*| To*| Call-Id| CSeq*
        |Contact* |User-Agent |Authorization |Event |Content-Length
        |Content-Type |Record-Route
INVITE_METHOD="INVITE"|%x49.4E.56.49.54.45
MESSAGE_BODY
additional rules
% content-Length%>0%
%content-Length%==size_of(MESSAGE_BODY)
(*) mandatory fields
```

Figure 8. Geneiatakis et al.'s detection signature for INVITE message

```
INVITE_METHOD SIP-URI | SIPS-URI MESSAGE HEADER+
MESSAGE HEADER=Via| Max-Forwords| From*| To*| Call-Id| CSeq* |Contact*
        |User-Agent |Authorization |Event |Content-Length |Content-Type |Record-
        Route
INVITE_METHOD="INVITE"|%x49.4E.56.49.54.45
MESSAGE_BODY
additional rules
% content-Length%>0%
%content-Length%==size_of(MESSAGE_BODY)
(*) mandatory fields
```

Figure 9. Geneiatakis et al.'s detection signature for SQL injection message

In addition to the two cited signature Geneiatakis et al have defined the SIP SQL injection detection seganture, which is illustrated in Figure 9. This signature allows to scanne and valid the data of Authorization field. Accordingly, the signature will validate the SIP syntax and corresponding headers contents (e.g. username, realm…). The validation of username and realm means that they will be scanned in order to determinate if they contain the SQL statements or not.

R. Ferdous et al. [6] proposed a new approch capable to classify SIP message as a "good" or "bad" depinding on whether its structure and content is acceptable or not. As

illustrated in Figure 10, a bad message can be a malformed, a crooced, or a malicious. R. Ferdous et al.'s framework constists on two stages filtringmethodologie. The first stage filtring is named the lexical analyser which is capable to extract the features from the incomming messages. Then, the exctracted information will be parsed in order to determinate if they are the part of the language by the formul grammar specified the SIP protocol. In the other hand, the second stage is called the structure and the content analyser, this stage is based on machine learning Support Vector Machines (SVM) [7] which has been proviouslytrainned to classify SIP messages by statistically learning from exemple of normal and abnormal messages.

In 2013, D. Seo et al. [8] proposed SIPAD: SIP-VoIP anomaly detection using a stuteful rule tree, the proposed work intends to secure SIP environment against malformed message attacks and flooding attacks. Seo et al. use an anomaly detection aproch by defining legitimate cases. The proposed aproach can identify unknown variant types of attacks. Furthermore, it doesn't need to maintain a large amount of attack signatures. SIPAD verifies whether the received messgematchs the pre-defined rules. In order to applay the RFC3261 rules, the authors translate the RFC3261 Augmented Backus Naur Form (ABNF) rules to regulare expressions. So, any incoming message that has unmatched or undefined headers is considered as undesirable message.

The rules defined by Seo et al. are based on the relationship between SIP messages, headers, and the states. These rules can adopt to a new standard by adding or modifing the existing rules.

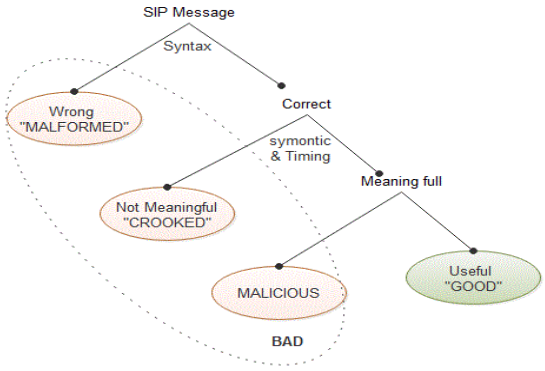


Figure 10. Simple binary classification of SIP messages

In 2015, Su and Tsai [9] proposed a new system framework which has two roles: the first is to filter malformed SIP messages that conflict with the SIP protocol, this role is affected by the malformed message detection module. The second role is to determinate whether the SIP server is under flooding attack or not. Such as the first module the message flooding detection module is responsible on the second role. To detected malformed SIP message attack Su and Tsai have used string comparison methode and used the methods proposed in [3, 18, 19]. So, any incoming message must firstly pass the first module which applies the RFC3261 SIP standard format as the basis for identifying malformed packet. Once a message is determined to be malformed the system updates the black list in the server database in order to block the future messages coming from the same source.

### 4.2. Comparison between Existing Solutions

In the Table 2 the advantages and limitations of each solution is shown. As we can remark each approch is based on different methode to detect SIP malformed message attack. Consequently, their advantages and limitations will be different.

Table 2. Comparison between some proposed approach

| Author's approach | Based on | Advantages | Limitations |
|---|---|---|---|
| Genieatakis et al.[2] | • Signature based on regular expressions | It w ok w ill with know n attack and w hen the signature attack exist in database | The rules defined cannot cover all type of malformed messages |
| Su et al.[9] | • String comparison | Simple | It cannot detect all various type of attack. |
| Firdous et al.[6] | • Syntax filter<br>• Learning machine SVM | It can detect and classify the type of malformed message. | Each message have to pass tw o stages<br>SVM has to be trained automatically and on real time. |
| Seo et al.[8] | • Stateful Rule Tree | The rules can adopt to a new standard.<br>Faster and efficient than the previous w ork. | - |

## 5. Conclusion

In this paper we have concentrated on SIP malformed message attack. After giving general information about SIP protocol, we have listed the different type of SIP malformed message. Then, we have classified their objectives and aims. In addition, we have analyzed the recent proposed works trying to detect the attack. Our analysis delivers the advantages and limitations of each approach.

For our future work, we will propose our proper approach which will be simple to implemented and efficient to detect SIP malformed message attacks.

## References


[1] Rosenberg J, Schulzrinne H, Camarillo G, Johnston A, Peterson J, Sparks R & Schooler E. SIP: session initiation protocol. 2002. (No. RFC 3261).

[2] Geneiatakis D, Kambourakis G, Lambrinoudakis C, Dagiuklas T & Gritzalis S. A framework for protecting a SIP-based infrastructure against malformed message attacks. *Computer Networks*. 2007; 51(10): 2580-2593.

[3] Niccolini S, Garroppo RG, Giordano S, Risi G and Ventura S. "SIP intrusion detection and prevention: recommendations and prototype implementation," In 2006. 1st IEEE Workshop on VoIP Management and Security. *IEEE*. 2006: 47-52.

[4] F Menna, R Lo Cigno, S Niccolini and S Tartarelli. "*Simulation of spit filtering: Quantitative evaluation of parameter tuning*". In IEEE International Conference on Communications (ICC '09). 2009.

[5] K Rieck, S Wahl, P Laskov, P Domschitz and KR Muller. "*A self-learning system for detection of anomalous sip messages*". in Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks. Springer Berlin / Heidelberg. 2008; 5310: 90–106.

[6] R.Ferdous, RL Cigno and A Zorat. "Classification of SIP messages by a syntax filter and SVMs". In Global Communications Conference (GLOBECOM), 2012 IEEE (pp. 2714-2719). *IEEE*. 2012.

[7] CJ Burges. "A Tutorial on Support Vector Machines for PatternRecognition". *Data Mining and Knowledge Discovery*. 1998; 2: 121– 167.

[8] D Seo, H Lee and E Nuwere. "SIPAD: SIP–VoIP anomaly detection using a stateful rule tree". *Computer Communications*. 2013; 36(5): 562-574.

[9] MY Su and CH Tsai. "An Approach to Resisting Malformed and Flooding Attacks on SIP Servers". *Journal of Networks*. 2015; 10(2): 77-84.

[10] Azrour M, Ouanan M, Farhaoui Y. SIP Authentication Protocols Based on Elliptic Curve Cryptography: Survey and comparison. *Indonesian Journal of Electrical Engineering and Computer Science*. 2016; 4(1): 231-239.

[11] Azrour M, Farhaoui Y, Ouanan M. A New Secure Authentication and Key Exchange Protocol for Session Initiation Protocol Using Smart Card. *International Journal of Network Security*. 2017; 19(6): 870-879 (DOI: 10.6633/IJNS.201711.19(6).02);

[12] Azrour M, Farhaoui Y, Ouanan M. (in press), Cryptanalysis Of Farash et al.'s SIP Authentication Protocol, *International Journal of Dynamical Systems and Differential Equations*.

[13] Azrour M, Farhaoui Y, Ouanan M. A server spoofing attack on Zhang et al. SIP authentication protocol.*International Journal of Tomography &Simulation*. 2017; 30(3): 47-58.

[14] Cai Z, Zhang Q, Li M, Gan Y, Zhang J. Multi-Domain Authentication Protocol Based on Dual-Signature. *TELKOMNIKA. Telecommunication Computing Electronics and Control.* 2014; 13(1): 290-298.

[15] Wei J, Liu W, Hu X. Secure and efficient smart card based remote user password authentication scheme. *International Journal of Network Security*. 2016; 18(4): 782–792.

[16] Geneiatakis D, Dagiuklas T, Kambourakis G, Lambrinoudakis C, Gritzalis S, Ehlert S, Sisalem D. Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys and Tutorials*. 2006; 8(1-4): 68-81.

[17] Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A, Stewart L. HTTP authentication: Basic and digest access authentication. 1999. (No. RFC 2617).

[18] Geneiatakis D, Lambrinoudakis C. An ontology description for SIP security flaws. *Computer Communications*. 2007; 30(6): 1367-1374.

[19] Geneiatakis D, Lambrinoudakis C, Kambourakis G. An ontology-based policy for deploying secure SIP-based VoIP services. *Computers & security*. 2008; 27(7): 285-297.