International Journal of
Soft Computing and Software Engineering (JSCSE)

Vol.4,No.2, 2014
Published online: Feb 25, 2014

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v4.n2.1

A New Approach to Authentication Mechanism in IP Multimedia Subsystem

Farzad Fekrazad

Department of Computer Eng., Islamic Azad University, Tehran Central, Iran

E-mail: ffekrazad@gmail;com

Abstract. **Regarding integrity in infrastructure networks and implementing IP Multimedia Subsystem (IMS) architecture, security has found considerable importance. IMS uses two signaling protocols named Session Initiated Protocol (SIP) and DIAMETER. In this paper we concentrate on SIP. Since SIP is an open source protocol and does one-sided authentication, it is vulnerable. In this paper we propose a Mutual authentication mechanism in SIP. In this approach, we eliminate the problems in HTTP Digest Authentication. This method protects the network against offline guess attack and man-in-middle replay attack. In our method we use 3 optional parameters such as cnonce, qop and next-nonce (nc). After that, to have a reliable connection we authenticate server. In order to evaluate our method we compared it with 4 routing principals of Tsai, Yang, Durlanik and HTTP Digest. We did the comparison considering parameters such as overhead, decoding time, compilation time, call delay, answering time and detection time. Though, we have decreased them comparing to Tsai, Yang and Durlanik. We have improved call delay by 30% compared to Tsai and lessen answering time by 50% comparing to Yang and Durlanik. When considering attacks, we found number of successful attack has decreased on average of 30% compared to all 4 methods.**

Key words: *mutual authentication, IMS, SIP server, vulnerability.*

* Corresponding Author: farzad fekrazad
Full Name,farzad fekr azad
Faculty of Electrical and Computer Science,
Azad University Tehran, Iran,
Email: ffekraza@gmail Tel:+989122886860

1 Introduction

IMS is a standard architecture network core which is able to support different terminals and different access approaches. It is introduced as next generation architecture. IMS is regarded as an evolutionary architecture. It uses SIP to take advantage of packet switch networks. The main component of IMS architecture is Call Session Control Function (CSCF) which are categorized in 3 groups including Call Proxy Session Control Function (P-CSCF), Serving Call Session Control Function (S-CSCF) and Interrogating Call Session Control Function (I-CSCF) [1]. SIP is a text-based protocol which is the basic element of real time applications such as VOIP, IMS and IPTV. It is an application-layer protocol. Messages in SIP are similar to Simple Mail Transport Protocol (SMTP).

Up to now different methods have been suggested to solve authentication problems in SIP. Some of them are noticed in following. Authentication is based on Diffe-Hellman [2]. It was resistant to offline guess attacks, replay and server spoofing. It has high computational overhead, hash functions and XOR operators. It does not need authentication in all SIP messages.

Another method was suggested in [3] to improve SIP Authentication which was based on ECDH.

Another principal was proposed in [4]. It was resistant to offline guess attack, replay attack and server spoofing. It had less computational overhead than [3]. Regarding high processing overhead, it was not suitable for weak devices.

Another approach was proposed in [5] to refine previously suggested methods in [3,4]. It was based on a random number. All of the communication messages were produced using hash functions and XOR operator. So, it had less calculation overhead. It was resistant to replay attack and server spoofing.

This paper consists of following sections: section 2 discusses related works, proposed method is presented in section 3, implementation is discussed in section 4.

2 RELATED WORKS

In this paper, we propose a new approach to refine the authentication mechanism in IMS regarding SIP communicational protocol. In our method, we take advantage of optional SIP parameters. First of all, we take a look at the method recently used in SIP authentication called HTTP Digest discussed in [6]. HTTP Authentication discussed in RFC 2617 is a form of HTTP Digest [6].

This mechanism is based on HTTP client-server. HTTP authentication uses two approaches in authenticating a user which are basic and Digest authentication.

Basic authentication is not used in SIP, because username and password are sent open source in this method. It is used in Digest SIP authentication by MD5 algorithm. In this algorithm, after sending REGISTER request by UA, SIP creates challenge. It returns 401 Unauthorized answer using “www-Authenticate”. Fig. 1 shows a sample example of using MD5.

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP
137.194.192.237:5060;received=137.194.192.237
From: <sip:ahmed@enst.fr>
To: <sip:ahmed@enst.fr>;tag=as7b4af592
Call-ID: D8A5240D579C4D6E8CE1@enst.fr
CSeq: 7168 REGISTER
User-Agent: Asterisk PBX
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE,
REFER,
SUBSCRIBE, NOTIFY
Max-Forwards: 70
Contact: <sip:ahmed@137.194.192.228>
WWW-Authenticate: Digest realm="asterisk",
nonce="64d45b88"
Content-Length: 0
```

Figure 1 MD5 Algorithm

Client uses “nonce” to answer. The answer is
created using username, password, method name, “Request URI”, nonce and realm. Nonce is found using formula in RFC 2617 which can be found in [6].

```
H(A1) = MD5(username”:”realm”:”password)
H(A2) = MD5(METHOD”:”Request-URI)
Response = MD5(H(A1)”:”nonce”:”H(A2)
```

Figure 2 shows finding nonce response

Password is found by username when creating SIP account.

Proxy server uses a mechanism, which is near to client. It creates its Digest to compare it with the sent Digest by client. If these two values are the same, the server authenticates the client.

But this mechanism has two major weaknesses. First of all, parameters and headers in SIP are not complete.

Second problem is distributing public keys because there is not a safe environment [7].

The proposed mechanism should be considered regarding the minimum effect in client side and minimum overhead while it can be implemented in IMS. It should also reduce the stated problems. For instance, a suggestion is to create a security center for distributing keys and changing authentication mechanism using these center accessories in IMS networks [8]. This idea has a big problem which is the need to changing the infrastructure. Since this idea is expensive, it is not good for implementation.

In all methods in networks based on client-server, authentication is done one-sided and this causes security challenges. SIP provides a challenge mechanism which is similar to authentication in HTTP [9]. This method uses MD5 hash functions to combine username and password which is known as HTTP Digest Authentication. When client establishes a connection with a proxy server, proxy sends proxy authentication requirement 407 for authenticating user. The user sends user authentication client 401. An example of WWW-Authenticate in 401 challenges is shown in Fig. 3 [6].

WWW-Authenticate :Digest
realm="biloxi.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
opaque="5ccc069c403ebaf9f0171e9517f40e41",
algorithm=MD5

Figure 3 WWW-Authenticate

A mutual authentication mechanism is proposed for authenticating by a middle proxy [10].
After the client receives challenges no. 401 or 407 from server, it send requests containing authorization header in response to 401 or proxy-authorization in response to 407. An example of authorization is shown in Fig. 4. Proxy-authorization has similar parameters.

Authorization: Digest username="bob",
Realm="biloxi.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f40e41"

Figure 4 Proxy-Authorization

In previously implemented methods, nonce played the main role in authenticating client and server in SIP protocol. Its value is related to implementation.
HTTP Digest, the recent powerful authentication approach, contains time stamp. Time stamp lets the similar values of nonce to be repeatedly used in serial and non-serial processes before time stamp expires. This is a problem. Since, one-time nonce is found by illegal people, it is possible that network security is threatened. Another problem regarding nonce is that, if the attack can use and remember the none-expired nonce, it causes replay attacks. So, if SIP is not protected against replay attacks, server should produce one-time nonce and forbid reusing it. One of the methods of producing such nonce values is using Authentication-Info or Proxy-Authentication-Info which also contains next nonce which is used by client in next request [11]. Parallel requests cannot be processed by server. If each answer contains one next nonce, client should use it in next request. So, implementation should regard tradeoff between performance and security. Usually, an old nonce value is allowed to be used repeatedly in a short period of time [12]. It is important that using one-time nonce is difficult since each time producing it has negative effect on server performance. It increases computational overhead on server.
So we should think of the way such that it uses values which are resistant to replay attacks and does not affect server performance.
Considering the related works discussed, SIP is very vulnerable. It demands more research and effective methods. This is the reason, we implement mutual authentication. The novelty of our method is finding a method to authenticate server regarding authenticating client. This will be discussed in next section.

3 PROPOSED METHOD

In order to have a mutual authentication, we use qop, nonce-count and cnonce which are produced in client and server. Suggested method solves the problems in current authentication. We make use of 3 SIP optional parameters.
We use qop to increase the security level of server. Cnonce is a random variable produced in client by receiving qop. It helps server to authenticate client.
Nonce-count (nc) is a nonce counter [13]. Cnonce is produced in client side while nc and qop are generated in server. We also use hash and MD5 algorithm to encrypt parameters which are sent from server side.
In our method, to prevent server spoofing, replay attack and offline guess attack, client should identify server.
The proposed approach is described as follows

1. Client sends an invitation message to server for making a new session.
2. Server produces qop, nonce,next-nonce (nc) and server IP. A copy of these values is kept in server

side. This created package is encrypted by MD5 hash functions. This procedure is shown in Fig. 5. It will then be sent to client side.

```
Authenticate :Digest
realm="biloxi.com",
qop"=auth,auth-int,"
nc=00000001
IP="X.X.X.X",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093"
,
algorithm=MD5
```

Figure 5 producing parameters in server

3. After receiving the packet produced in previous step, client decrypts it. It extracts qop. Then, client produces cnonce. It makes a copy of cnonce, qop, nc, nonce and server IP. If the package does not contain qop, cnonce is not produced in client.
4. Then client creates a new packet containing qop, nc, cnonce, nonce and client IP. This new package is encrypted by MD5 hash functions. This can be found in Fig. 6.

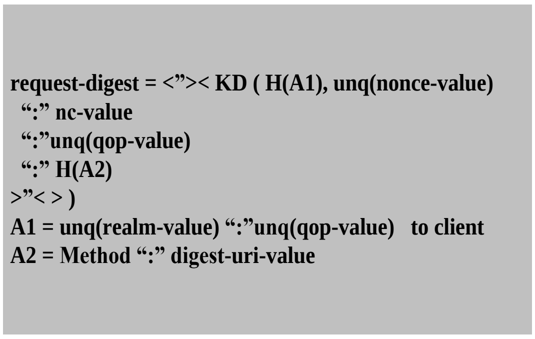
```
Authorization: Digest username="",
          Realm="biloxi.com",
          nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093"
          qop=auth,
          nc,00000001=
          IP"=X.X.X.X,"
          cnonce="0a4f113b",
              algorithm= MD5,

response="6629fae49393a05397450978507c4ef1",
```

Figure 6 producing parameters in client

5. Server decodes packet created in step 4, then it takes out cnonce and client IP. Server compares nonce, qop and nc with values stored in step 2. If nonce, qop and nc are equal to values in step 2, client is authenticated to server.
6. Then server sends message 200ok by cnonce, nonce, nc, server IP and qop to client.

7. When client receivers the produced package in 6, client compares cnonce, nonce and qop with values in 3. If cnonce, qop and nonce are equal, client authenticates server.



```
request-digest = <"">< KD ( H(A1), unq(nonce-value)
  ":" nc-value
  ":"unq(qop-value)
  ":" H(A2)
>"< > )
A1 = unq(realm-value) ":"unq(qop-value)   to client
A2 = Method ":" digest-uri-value
```

Figure 7 authenticating server to client

8. Client sends 200 ok to server and the session starts.

By this algorithm, mutual authentication is implemented. Fig. 8 shows the proposed algorithm.

4 SIMULATION

In order to evaluate our method, we compare our results with The popular algorithms such as HTTP Digest, Tsai, Yang and Durlanik. Our comparison considers number of successful attacks overhead and several things els that shown in table 1.

According to Tabel 1,Decoding time has decreased compared to Two methods (Tsai and Yang). Compiling time in proposed method is equal to HTTP DIGEST and Durlink which is less than Yang and Tsai. Attacker can find the password after thirty two times tries which shows improvement compared to HTTP DIGEST, Tsai, Yang and Durlanik.

According to our algorithms shown that Detection time has decreased down to fifty percent and Answering time has reduced fifty percent to compared to Tsai,Yang and Durlanic. Number of successful attacks have decreased about 30 percent.

5 Conclusions

In this paper, we investigate and analyze the methods for improving authentication in IP Multimedia Subsystem environment for NGN network. We proposed A New Authenticated Mechanism in IP Multimedia Subsystem. It helps to prepare a network secure environment without any changing in network infrastructure. The main advantages of the proposed method include mutual authentication, integrity, message freshness, preventing server spoofing, implementing a secure key center and compatibility.

We tried to find a method which does not change infrastructure. It should also reduce the probability of replay attack comparing to other mechanisms and prevent server spoofing. In order to evaluate our method, we compared it with HTTP Digest, Tsai, Yang and Durlanic. We can increase decoding time and compilation time but we did not increase another paramiter same as overhad in our method. We can also improvment another parameter same as Non of successful attacks down to compared to HTTP , Yang and Durlanic . In our method the Non of accidental attack detection are without any. In our method the Non of accidental attack detection are without any changes. This proves the effectiveness of our method.

Table 1 Comparison of proposed method with previously proposed methods

Durlanik	**Yang**	**Tsai**	**HTTP DIGEST**	**Proposed Mechanism**	
0.04	0.04	0.02	0.01	0.01	**Overhead**
0.2	0.4	0.3	0.02	0.01	**Decoding time**
0.2	0.4	03	0.2	0.1	**Compiling time**
30st	30st	30st	27st	32st	**Man in the middle attack**
0.40ms	0.07ms	0.08ms	0.02ms	0.03ms	**Detection time**
0.06ms	0.06ms	0.04ms	0.05ms	0.03ms	**Answering time**
8	8	8	8	8	**Non of accidental attack detection**
5	6	5	5	2	**Non of successful attacks**

e-ISSN: 2251-7545
DOI: 10.7321/jscse.v4.n2.1

References

[1] T. Russell, The IP Multimedia Subsystem (IMS) Session Control & Other Network Operations, published by Mc Graw Hill,2008.

[2] M. T. Hunter. "Security issues with the ip multimedia subsystem (IMS)," in Technical Report TS 33.978 V7.0.0, pp. 1-6, June.2007.

[3] Aytunc Durlanik, Ibrahim Sogukpinar, "*SIP Authentication Scheme using ECDH*", 2005

[4] J. L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," International Journal of Network Security, vol. 8, pp. 312-6, 2009.

[5] 3GPP TS 24.229 V9.3.1 (2010-03) ,3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 9).

[6] F. Wang and Y. Zhang, "A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography," Ankara,Turkey,Computer Communications, vol. 31, pp. 2142-2149, Aug 2008.

[7] M. Maachaoui., "Model based security analysis for IMS network," *in Multimedia Computing and Systems (ICMCS), Ouarzazate,* Taiwan pp. 1-6, April. 2011.

[8] C. Y. Chen., "Transaction-Pattern-Based Anomaly Detection Algorithm for IP Multimedia Subsystem," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 152-161, 2011.

[9] I. Vidal, et al., "Evaluating extensions to IMS session setup for multicast-based many-to-many services," Computer Networks, 2010.

[10] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, H. Schulzrinne, SIP Security, published by Jhon Wiley,2009.

[11] 3GPP TS 33.203 V10.0.0 (2010-06) , 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services (releases 10) ,2010.

[12] T. Guillet, et al., "Mutual Authentication for SIP: A semantic meaning for the SIP opaque values, "Turin, Italy, pp. 1-6, Feb2008.

[13] "network technology .meta switch". Internet: www.AVISPA.org/ , [Nov. 14, 2011].