J. Basic. Appl. Sci. Res., **2(9)9378-9382, 2012**

© 2012, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied
Scientific Research
www.textroad.com

2 Way Authentications for IMS by ECDH

Maisam-Mohammadian[†1]Nasser-Mozayani[2]

[1]Department of Computer Eng., Iran University of Scienceand TechnologyNarmak, Tehran Iran
[2]Assistant Professor at Department of Computer Eng., Iran University of Science and TechnologyNarmak, Tehran, Iran

ABSTRACT

Communication between IP multimedia subsystem (IMS) servers is done based on Session Initiation Protocol (SIP). SIP is an application-layer control operating on top of a transport protocol which allows creating, modifying, and terminating sessions among more agents. For authentication, SIP relies on HTTP Digest by default; the client is authenticated to the SIP proxy server. In this paper we propose a mutual authentication mechanism that is not based on HTTP Digest and then, we implement our method in IMS and compare our results with the existing results based on intruder. We found that our proposed mechanism has more stability against intruder and unauthorized access. In this paper we introduce a new approach for user authentication or server authentication by using Elliptic curveDiffie–Hellman (ECDH) and optional SIP's header. Through our solution we can protect any network such as IMS network from intruders and eavesdropping. In our solution we can increase necessary steps for intruder to decode authentication.

KEYWORDS- IMS network; SIP; Security; HTTP Digest; AKA.

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 is 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). SIP uses a several parameter for send and receive all of the request messages that including invite, bye, Ack, cancel each of them uses between clients and servers. More explanation can be found in the RFC3261,2617, 2616, 2613 document [2,3]. Up to now different methods have been suggested to solve authentication problems in SIP. Some of them are noticed in following, because most of protocols create interoperability problems. Regarding high processing overhead, it was not suitable for weak devices[4] Since the authentication based on HTTP Digest mechanism is one of SIP weakness, This paper suggests a novel approach to increase reliability in authentication which will be discussed. This problem is one way authentication and we will be use solve this problem by ECDH in IMS network.In this paper we will present SIP authentication mechanism in section 2 andProblems in SIP authentication insection 3 and our solution overview in section 4 and simulation in section 5 and conclusion in final

2. SIP authentication mechanism

Sip is a general uses protocol for real time services. This protocol is very useful protocol for NGN communication. IMS that based on NGN network so Using authentication in IMS, there exist two generaland principles for providing security, first is end-to-end and second is hop-by-hop [5]. End-to-end security on SIP data involves end users, for example SIP authentication. In contrast to end-to-end technique solutions which use SIP mechanisms to ensure security, hop-by-hop method relies on the security provided by the network.In terms of authentication, we have several mechanisms and solution exist that include Durlanik, Yang and transport-level security and Tasithat uses in IMS network. In addition to those, we have other techniques of authentication in IMS security, which are designed to increase security in IMS protocol. The Hypertext Transfer Protocol Digest provides a challenge/response for each message and is uses by

***Corresponding Author:** Maisam-Mohammadian, Department of Computer Eng., Iran University of Scienceand TechnologyNarmak, Tehran Iran, E-mail: maisam1363@comp.

default MD5 algorithm [6]. As another side, some lightweight program such as has several problems. One part of the SIP that build 'response' is called 'nonce' this header is a random variable which is generated by proxy serve and is created using user name, method and password for response to operate as shown in algorithm 1. This is general algorithm for authentication[2].

- Authentication :Digest
- Nonce=”abdf123ke456c78w89t”,
- Realm=”iust.ir”
- Algorithm=MD5 (we will uses to this generate of MD5 in this part to H(A1) and H(A1))
- H(A1)=MD5 (username”:” realm”:” password)
- H(A2)=MD5(Method”:” Request-URI)
- response=MD5(H(A1) ”:” nonce”:” H(A2))

Algorithm1:general algorithm for authentication

3. Problems in SIP authentication

We have severalweaknesses in The Hypertext Transfer Protocol Digest, but in this section we have introduce twoimportant weaknesses in this authenticationthat uses in IMS protocol such as session Initiation protocol or diameter [7]In previously implemented methods, nonce played the main role in authenticating client and server in SIP protocol and don’t use The public key infrastructure is also susceptible to replay attacks. HTTP Digest, the recent powerful authentication approach, contains time stamp.[8] 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. Another side in previous solution all authentication mechanism use one parameter that this is a major weakness in sip protocol how use in IMS model.[9]

4.Our solution overview

In this section, we explain our method. According to explanation in previous section, we used two more items in our approach to increase authentication security in the networks that are based on SIP communication. We used “Cnonce” and “ECDH” in our method and compared our results from different aspects to basic communication networks such as IMS networks. We tested our idea by new software tools and compared our results with previously implemented results in IMS network which are currently working. This software called ’AVISPA’ this software is usefulfor security protocols check.“Cnonce” is an optional and random value used in SIP message packet and is explained in RFC 3261[12].First, when challenge message is received in user client, the client extracts that by private key and then, it generates a new random value that we call response according to (1). This value is generated in the proxy server by another algorithm which will be explained later in this section. The user agent uses Elliptic curve Diffie–Hellman (ECDH). The inputs for ECDH include public and private key and 2 mathematical equations which are shown in Algorithm 2;

1- A = Kpriv mod (N-2)
2- response = A. Kpriv+ NONCE
3- N= large string of value that is used for ECDH.

Algorithm2: ECDH Algorithm in client

Second, after the execution of the ECDH part,the random value generated is called Response. In next step wefetch SIP messages and encrypt them by this value. The other side in the server proxy uses the algorithm (2) to make qop. Next step Theqop is calculated in the proxy server by this algorithm (3).

- request = KD (H(A1), unq(nonce-value)“:” nonce count-value“:” unq(cnonce-value)
- A1 = unq(username-value) “:” unq(realm-value) “:” password
- A2 = Method “:” digest-uri-value
- qop=”auth”,request-
- Cnonce= Kpriv+qop

Algorithm 3: Cnonce genareate

Upon message is received by server, the server starts to decode the message and compare the Cnonce and qop note (this vales are random parameter). This algorithm is shown in (3) and shown is flowchart in fig 1. If these two parameters are the same, the user is authenticated to the server.This model can be used for mutual authentication which we tested this idea in mutual authentication by AVISPA tools.

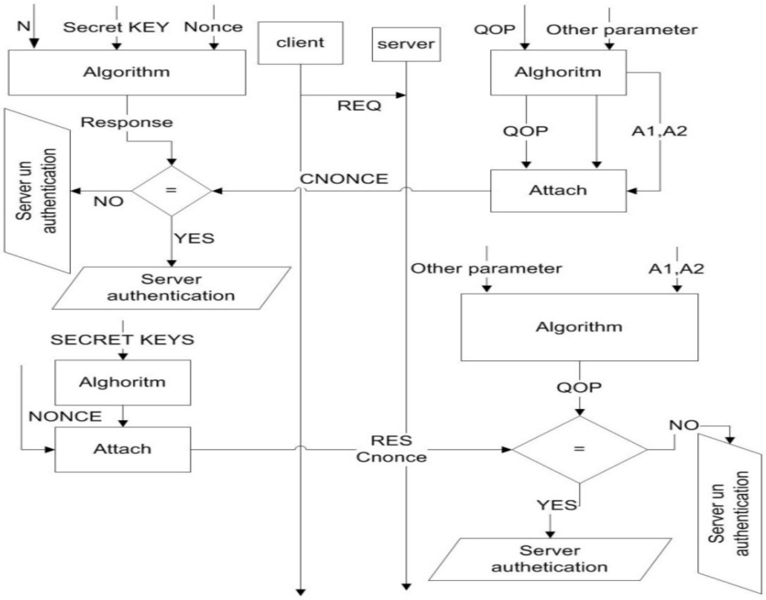

Figure1: proposed authentication enhancement mechanism

5. SIMULATION AND RESULT

In order to evaluate our method, we used Automated Validation of Internet Security Protocols and Applications (AVISPA). This software has been developed by AVANTSSAR [13]. This software contains reach library which contains popular protocols in authentication. It also provides simulation environment which has the ability to define different attacks. We compare our results with 4 most popular algorithms such as Tsai, Yang Our comparison considers overhead, decoding time, compiling time, call delay, detection time,pars time, answering time in table1. We also studied attacks such as man in the middle, server spoofing and offline guess attack. We compared our results with HTTP Digest [14], and IPsec. We also found actual amount of throughput and compared it by Kong et al [10] solution which is presented in the Table1 [16].Detection time has decreased down to 50% compared to Tsai. Answering time has reduced about 50% compared to Yang and Durlanik. Number of successful attacks has decreased about 30% on average compared to 4 stated algorithms.

According to Table1, when considering overhead, proposed method has equal overhead compared to HTTP DIGEST. It has less overhead than Tsai, Yang and Durlanik. Decoding time has decreased compared to Yang and Tsai. Compiling time in proposed method is equal to HTTP DIGEST and Durlink which is less than Yang and Tsai. Call delay has a reduction of 30% compared to Tsai and Yang.. Man in the middle can find the password after 32 steps which shows improvement compared to HTTP DIGEST, Tsai, Yang and Durlanik

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	0.02	Decoding time
0.2	0.4	03	0.2.	0.2	Compiling time
0.35ms	0.40ms	0.40ms	0.14ms	0.10ms	Call delay
0.07ms	0.04ms	0.03ms	0.05ms	0.01ms	Pars time
5 stage	4 stage	4 stage	5 stage	4 stag	Analyze
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	Answer time

5. Conclusion

In this paper, we investigate and analyze the methods for improving authentication in IMS environment based on SIP protocol. We proposed a mutual authentication mechanism. This algorithm tries to remove SIP authentication weaknesses. It helps to prepare a secure environment while preventing changing 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 Pars time comparing to other mechanisms and prevent server spoofing. In summary, it increases authentication reliability in IMS. In order to evaluate our method, we compared it with HTTP Digest, Tsai, Yang and Durlanik. We did not increase overhead, decoding and compilation time. We also decrease detection time down to 50% compared to Tsai. Answering time has decreased about 50% compared to Yang and Durlanik. Number of successful attacks has decreased about 50% compared to Yang. This proves the effectiveness of our method.

6. Future Work

In future, we plan to test our method for multi domain network. We will also consider more attacks and check this solution for other models such as S/MIME and DTLS. We will also check this method for email security and IMS2.0

REFERENCES

[1]J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, “SIP: Session Initiation Protocol”, RFC 3261, June 2002: http://www.ietf.org/rfc/rfc3261.txt..

[2]M.mohammadian and N.mozayani“A New Mechanism For Mutual Authentication In *SIP“International Journal of Computer Science Issues”*May 2012 Volume 9, Issue 3.

[3] Liao YP, Wang SS. “A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves”. *Computer and Communications* 2010; **33**(3):372–380.

[4] P. Urien, “TLS Tripartite Diffie-Hellman Key Exchange*”, IETF draft (work in progress), July 2010.*

[5] RFC 4492, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", *May 2006.*

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

[7] W. Werapun, A. A. El Kalam, B. Paillassa, J. Fasson," Solution Analysis for SIP Security Threats", *The IEEE international Conference on Innovations In Inforamtion Technology(IIT'08), 2008.*

[8] B. Li,D. Wang, S. Zhang, " Policy Based SIP Signaling Management in IMS", *Alcatel-Lucent 1-6/F Sec. D Hi-Tech Software Park Qingdao, 266101, China2009.*

[9] A. Nemi, J. Arkko, V. Torvinen, " *Hypertext Transfer Protocol(HTTP) Digest Authentication Using Authentication and Key Agrement(AKA*),IETF RFC 3310, 2002.

[10] Kong L., Balasubramaniyan V.B. and Ahamad M. A lightweight scheme for securely and reliabl.

[11] M. Sher, T. Magedanz, "Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)" *,IEEE First International Conference on Availability, Reliability and Security (ARES'06), Austria, 2006*

[12] F. Leitold, A. Medve, L. Kovacs, " SIP security problems in NGM Services ", *The IEEE International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST'07),2007*.

[13]http://www.avispa-project.org/ validate in 2005 by IETF.

[14] . Tsai JL. "Efficient nonce-based authentication scheme for session initiation protocol". *International Journal of Network Security* 2009; 8(3):312–316.

[15] .Yoon E, Shin Y, Jeon I, Yoo K. "Robust mutual authentication with a key agreement scheme for the session initiation protocol".*IETE Technical Review* 2010;**27**(3):203–213.

[16] T. Dierks, E. Rescorla, The Transport |Layer Security(TLS) Protocol Version 1.2, 2008.