International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012

DOI: 10.7321/jscse.v2.n9.3

# Improving of Authentication Mechanism in IMS Environment By Integration Hop By Hop And End To End Model

[1] Maisam Mohammadian, [2]Nasser Mozayani,
[1*] *Msc Student, IUST, Iran*
[2] Nasser Mozayani *Assistant professor, IUST, Iran*
*Email:* [1]*maisam_mohamamdian@yahoo.com*, [2] Mozayanii@iust.ac.ir

***Abstract.*** **SIP protocol is the standard signaling that developed for multimedia services and the interface between IMS servers and Existence defined. Integration of telecommunication networks and increase services based on sip protocol, we will feel more the need to increase the security level of this protocol. As current sample security mechanisms can be pointed to the End To End and Hop By Hop. In this manuscript we combination End To End and Hop By Hop models and present new model that called Hybrid. our propose based on mathematic relationship and new installation key. We implementation our propose by AVISPA software and then compare all of the result same as procedure time, overhead insure device and security holes that exit in, this model compared to previous models has been improved by this model**

**Keywords**: *IMS network, hybrid model, mutual authentication*

* Corresponding Author
Maisam Mohammadian
*Msc Student, IUST, Iran*
*Email:maisam_mohamamdian@yahoo.com*

## 1. Introduction

Session Initiation Protocol (SIP) is a signaling standard approved by IETF(Internet Engineering Task Force) for real time .multimedia session base on ims network. Establishment Increasingly wide deployment brings much concern on SIP Security Current solutions for end-to-end signaling security either require user-side powerful performance support for heterogeneous security mechanisms, or assume that trust relationship is transitive and static.
Another side this protocol use for Negotiation between IMS Existence network. Yet no solution is suitable for weak terminals with inherent computational power limitations. It is necessary to consider a reasonable combination of security solutions could be provided by the end users and the network servers. This paper presents a hybrid security model, combining hop-by-hop and end-to-end security, that trusted neighbor servers help weak terminals to make end-to-end communication secure with lightweight overload. SIP supports hop-by-hop security using Transport Layer Security [6] and end-to-end security using Secure MIME (S/MIME) [7]. Hop-by-hop security assumes that a SIP user agent trusts all proxy servers along its request path to inspect the message bodies contained in the message while end-to-end security assumes that a SIP UA does not trust any proxy servers to check the message [2,1]. Hop-by-hop security cannot prevent attacks from malicious intermediaries while end-to-end security provides higher degree of security and better level of performance.

Some of the existing security solutions [3,4] for end-to-end communication are designed based on hop-by-hop security with insufficient security. Others do not consider the inherent limitations of weak terminals such as mobile phones which appears a promising application of SIP. Our propose implement a security light Wight with high efficiency is where users with the ability to use equipment that is weaker and further opportunity to provide lower permeability.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

The End to end authentication mechanism that the main purpose is only the beginning and the end user in a session have access to content and meaning of a message, and intermediate agent Can not ability to access and modify the packets sent to user. In this kind of communication to establish and develop confidentiality and security protocol to integrate data form S/MIME is used[5,6]. End to end approach is to have some major problems in the implementation of this method that is not used much more.

Today another mechanism popular that is used is based on hop by hop. This method of authentication, have placed is network layer and is used from regular security model for confidentiality and data integration same as IPSec and TLS. In this model we will have problems that such as heavy overhead on the user equipment and the middies way equipment who the passes the packets[7,8].

## 2. Hybrid Model in IMS Architecture

We are present a new model that called hybrid that based on Lightweight key and make new installation key. In this solution we will used from a new assumption that user trusts the first next-hop server and trusts an opposite-side user via transitive trust another word that the next server is safe of any attack. We want named next hop server neighbor servers. This agent act same as security agent for share overload for wake terminals. We also assume that a hierarchical CA system exist for intermediate servers. In most cases, servers are much stable than UAs so that it is easier for intermediaries to build a hierarchical CA system. This solution is suitable for IMS architecture because this propose can handle all heavy load user without have nothings effective on user equipments. Because we transfer all heave load to nighters server who is trust for own domain. In previous models for the sharing of security mechanisms of a first Identifier. But In this paper, rather than the identifier of the neighbor on the server will use to build confidence The key is to be installed in the IMS network will use to implement[11,12].

## 3. Components of suggested model

According to the test in frame work at the lab and on the android phon and compared with compiletion time and pars time, We will suggestion this solution because is very suitable and light weight for smart phone and portable devices. In this way we use public and private keys, and also take inspiration from the math above the resistance level of the system. In this method, keep in mind that the computational overhead is lower than the previous methods. Methods on a common framework for encryption research and testing on mobile devices and are derived the results of this paper .

Alice as a user agent choose a random sequencer that called (r) and calculated the amounts of $g^2 \bmod p$ and $g^{h(pwd)} \bmod p$ saves them as three effective amounts. The Pwd user password and h are also a hash function for one way authentication. Alice makes a random sequence that will name $N_A$ and will calculate the relative amount by H(pwd) +r+ $N_A$ The random amount of $N_A$ will be regenerated when the user agent had operated the authentication and the agreement key. The $g^{h(pwd)} \bmod p$ and $g^2 \bmod p$ amounts will have the ability to reuse and reduce the computational level for weak terminal users. The Sip server begins to calculate the amount of $g^{h(pwd)+N_A+r} \bmod p$ and following that will find the $g^{N_A+r} \bmod p$ amount of with the help of relation (1) when it receives the Register or Invite message. Here we point out that the detector of user password is already stored in the server to calculate $g^{h(pwd)} \bmod p$ .

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

$$(1)\ g^{N_A} \bmod p = \frac{g^{h(pwd)+N_A+r} \bmod p}{g^{h(pwd)} \bmod p + g^{r} \bmod p}$$

Then server choose a sequence random number we called $N_S$ and with $g^{N_S} \bmod p$ the help of begins to calculate the necessary key. From then on the server will start sending the regular message of 401.

In the user agent part, the 401 challenge message is received and it begins to calculate the main key with $g^{(N_S)N_A} \bmod p$ the relationship in the user authentication of our desire. Similarly, the operation will be.

performed inside $g^{N_A} \bmod p$ the server and that results in the production of user agent's key. It is noticeable in this approach that the user agent performs the mathematical calculations only once and if in this case it is consistent with the defined parameters , then the server in the first step will ensure greater with the user agent.

All these relations are based on the authentication in the hop mode and the result would be able to move Trust Dynamically as an authenticated package on any type of authentication protocol without worrying for weakness in the terminals. These points should be noted that the user agent has a AK key and a EK and MK key according to the following relation:

(2)
AK= H(MK" authentication key")
IK= H(MK" integration key")
EK=H(MK" Encryption key")

(EK) and (IK) in relation (2) are used to maintain SIP key between user agent and server. But we use relation (3) for license approval.

(AK) is used to recognize user and if everything that concerns in all required parameters for authentication of a system is equal, then it sends a S1 respond for mutual authentication with the sending detail given in relation (3):

$$(3)\ response_{A1} = H(AK \,||\, g^{h(pwd)}, Nonce1 \,||\, realm \,||\, Username \,||\, g^{N_S} \,||\, g^{N_A})$$
$$response_{S1} = H(AK \,||\, g^{h(pwd)}, Nonce1 \,||\, Nonce2 \,||\, realm \,||\, g^{N_S} \,||\, g^{N_A})$$

When a user agent to send a registration or call request, the user agent and the manufacturer server produce an effective amount of , $response_{S1}$ $response_{A1}$ in order to use AK. Here we need another amount that must be in the key and we use Next nonce parameter. SIP messages are usually kept by (Ek) and (IK) in a Hop by Hop method.

In the method that we are presenting in this paper, we comb in the two models of end to end and the Hop by Hop and, with utilization of the new installation key which we call N', we achieved good

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

results in load processing and security holes. This Key is essentially defined to keep the timing in sending and receiving and the base key lifetime which is defined as default time. Therefore, following the key loss by the end of its lifetime according to definitions in RFC3261, RFC2617, we can conclude that this key is implementable on both authentication mechanisms with very low overhead on the equipments [10].

(4) H(Pwd)+N'+r

Finally in this method, which is a combination of two models of authentication and encryption of data, before the meeting three principles of operation are done. With the help of these three principles, the combination of the two expressed authentication models are made possible.
These three principles are:

1) $g^{h(pwd)+N_A+r} \bmod p$
2) $g^{(N_S)N_A} \bmod p$
3) $g^{N_S} \bmod p$

The Operations $g^{h(pwd)+N_A+r} \bmod p$ and $g^{N_S} \bmod p$ begins with the receiver of invitation message. As soon as the message $response_{A1}$ is received, server $g^{(N_S)N_A} \bmod p$ begins to operate.

The advantages of this method $g^{(N_S)N_A} \bmod p$ is that we have the possibility. Finally we choose this model for this cause that is very suitable for use in IMS network and compatible to all of the NGN model.

## 4. Result

To reduce overhead by using the time of production of the new installation key. Nevertheless, it will prevent recycling attacks and guessing passwords through reduction of security holes. Relations we used here are with the help of AVISPA software and in order to measure the percentage of penetration of destructive factors, using (AKA) test and identifying security holes in end to end models and Hop By Hop.

In the method we used, we controlled the two models with the (AKA) input and save the required output. Then we tested our offer with the same input under the same conditions and we obtained the following results. These tables present workload of processor in described models and results are shown on a diagramming Figure 1.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

We finally concluded that the proposed hybrid model have a smaller work load on weaker equipment's comparing to other existing methods. On the other hand, by doing the test mentioned above and its results, the permeability of the proposed model is being tested and the results are presented in Table 2.

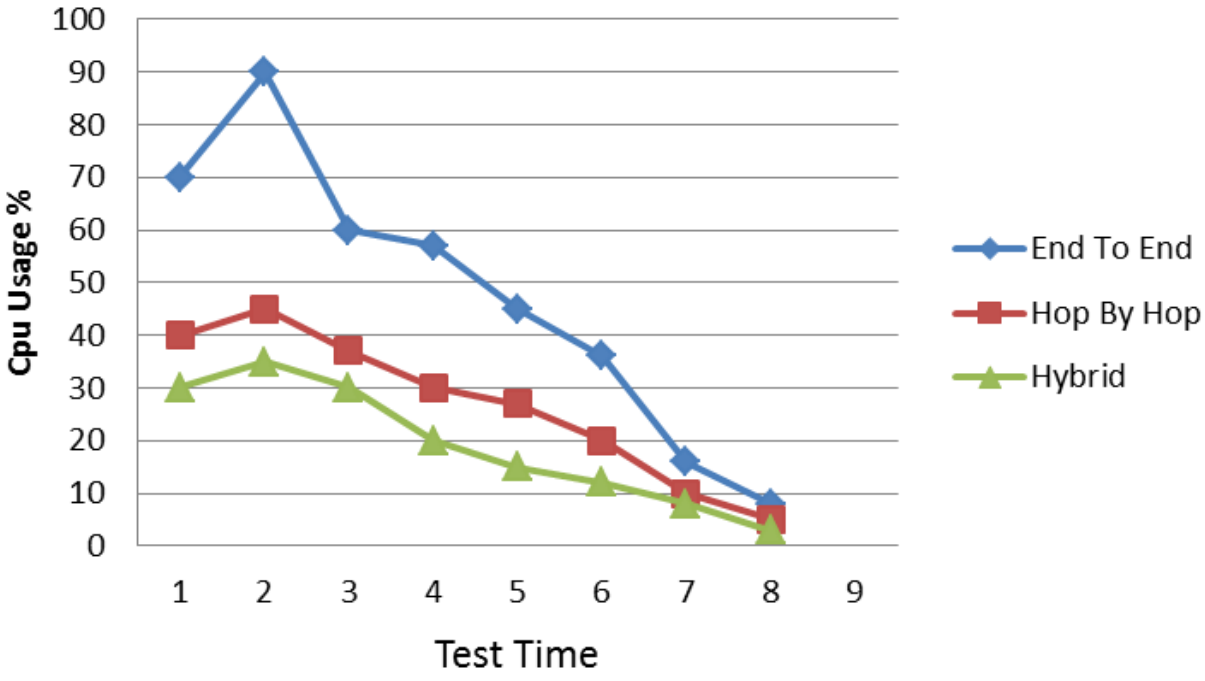


Figure1:cpu activity percentage in 3 model test.

In the following comparative table we have examined security holes in various models. The following table shows the results of comparison between, three security models in terms of response times to requests and delays in action time, implemented in a single program in AVISPA environment. All of the simulation codes are available if you contact to me. In table 3 you will found part of code uses.

Table 1: Action time comparison in 3 security models

| | Req1 | Ack | Delay |
|---|---|---|---|
| End to End | 4.203 | 4.204 | 0.014 |
| Hop by hop | 5.306 | 5.309 | 0.023 |
| Hybrid | 3.976 | 3.977 | 0.012 |

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

Table 2: code ssample uses for check by AVISPA

```
local IMS, Sid, Pa, PMS: text,

         Nb: text,
         State: nat,
         Finished: hash(hash(text.text.text).agent.agent.text.text.text),
         ClientK, ServerK: hash(agent.text.text.hash(text.text.text)),
         Kb: public_key,
         M: hash(text.text.text)

const sec_clientk, sec_serverk : protocol_id

init  State := 0

transition

   1.  State = 0
       /\ RCV(start)
       =|>
State' := 2
       /\ Na' := new()
       /\ Pa' := new()
       /\ Sid' := new()
```

## 5. Further work

In next paper we will try to implement this idea to smart phone and VoIP. Because we are believes to this idea that is suitable for implement to communication devices and we will implementation in new IMS network that have been call IMS 3.0.

## 6. Acknowledge

Authors want to thanks to Iranian Telecommunication Research center for ICT – ITRC for supporting this research work at IMS innovation Lab at ITRC-Iran-Tehran. Under this contract 5850/500/T

## References

[1] IETF RFC3329,j.Arkko,V.Torvinen, G. camarillo, A. Niemi, T. Haukka, Security mechanism Agreement for the Session Initiation Protocol(SIP), 2003.

[2] H. B. Fangqin and X. Huang,. "Authentication Key Exchange Protocol for IMS," *in Power and Energy Engineering Conference (APPEEC)*, Chengdu,China, pp. 1 – 4, March. 2011.

[3] 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.

[4] V. RodriguezandY.Donoso,., "Security mechanism for IMS authentication, using public key techniques," *Turin, Italy*, pp. 163-170, 07 October 2010.

[5] M. Gouda and M. Haggag, "Enhanced Authentication Mechanism for Next Generation Networks," *Beijen, China*, pp. 288-295,Jun. 2010.

[6] M. Z. Rafique, andKhan, M.K., "Securing IP-Multimedia Subsystem (IMS) against Anomalous Message Exploits by Using Machine Learning Algorithms,"*Bumbi, India*, 2011, pp. 559-563,Feb. 2011.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.9, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n9.3

[7] 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.
[8] C. C. Lee, "On Security of An Efficient Nonce-based Authentication Scheme for SIP," *International Journal of Network Security,*vol. 9, pp. 201-203, 2009.
[9] S. Zaghloul and A. Jukan, "Signaling rate and performance for authentication, authorization, and accounting (AAA) systems in all-IP cellular networks," *Wireless Communications, IEEE Transactions on,* vol. 8, pp. 2960-2971, 2009.
[10] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, H. Schulzrinne, SIP Security, published by Jhon Wiley,2009.
[11] IETF RFC3261,j.Arkko,V.Torvinen, G. camarillo, A. Niemi, T. Haukka, Security mechanism Agreement for the Session Initiation Protocol(SIP), 2006.
[12] R. Copeland, "Converging NGN Wireline and Mobile 3G Networks with IMS", CRC Press, Taylor & Francis Group, 2009.
[13] X. Fangmin, Z. Luyong, and Z. Zheng, "Interworking of Wimax and 3GPP networks based on IMS [IP Multimedia Systems (IMS) Jun. 2011.
[14] http://www.avispa-project.org/web-interface in 2011.