ISSN:0975-9646

A Proposed IP Multimedia Subsystem Security Framework for Long Term Evaluation (LTE) Networks

Samah Osama M. Kamel [#1], Adly S. Tag El Dein [*2], Nadia H. Hegazi [#3], Hala M.Abd El Kader [*4], Hany M. Harb[#5]

[#]*Research Assistant in Electronic Research Institute, Egypt, Giza*
[*] *Faculty of Engineering in shoubra,Egypt, Cairo*
[#] *Faculty of Engineering in Azahr University, Egypt, Cairo*

***Abstract*—An IP Multimedia Subsystem security Framework for Long Term Evaluation (LTE) networks with multimedia services is proposed. It is based on the packet switched (IP) protocols which provide the best effort service. The paper creates an architecture for deploying VoIP applications that provides for both QoS and charging, and for efficiently integrating multiple different services, which can be easily mixed and matched to meet the user needs. The IMS layers vulnerabilities are analyzed and security mechanisms to handle such attacks are presented. Therefore the paper presents two scenarios to handle such attacks.**

***Keywords*—Security, IP Multimedia Subsystem (IMS), Internet Protocol (IP), Session Initiation Protocol (SIP), Intrusion Detection and Prevention (IDP).**

I. INTRODUCTION

At present, cellular telephone networks provide services to over one billion users worldwide. Modern cellular networks provide messaging services ranging from simple text messages (Short Messaging Service (SMS)) to multimedia messages which may include video, audio, and text (Multimedia Messaging Service (MMS)). Cellular users are able to surf the Internet and read email using data connections, and some operators even offer location services which notify users when a friend or colleague is nearby.

The new framework IP Multimedia Subsystem (IMS) firstly is specified for mobile networks, especially for Universal Mobile Telecommunications System (UMTS) networks. It has been introduced and standardized by the Third Generation Partnership Project (3GPP) and the European Telecommunications Standards Institute (ETSI) providing Internet Protocol (IP) telecommunication services.

The idea of IMS is to offer Internet services such as the voice, data communication services, video conferencing, messaging and web based technologies everywhere, anytime, and with any terminals. The challenge of IMS architecture comes from this convergence by using cellular technologies. Any cellular user can access the Internet using a data connection utilizing any services the Internet may provide. IMS has then evolved to comprise several access technologies, including both wireless and wired networks. IMS has become a key enabler for the convergence of fixed and mobile technologies.

Compared to previous telecommunication infrastructures, IMS presents huge advantages such as easy development and deployment of new services, high level of quality of service, and common billing and charging functionalities. The IMS is derived from the fact that modern networks are primarily based on the packet switched (IP) protocols which provide the best effort service. The Goals of IMS are to create architecture for deploying VoIP applications that provides for both QoS and charging, and to provide architecture for efficiently integrating multiple different services, which can be easily mixed and matched to meet the user needs. The IMS specifications to be used by service provider to build multimedia services are concerned of standards of QoS, Charging and security.

IMS is overlay architecture to provide the Long Term Evaluation (LTE) networks with multimedia services. User Equipment (UE) needs a new IMS Subscriber Identity Module (ISIM) located within the Universal Integrated Circuit Card (UICC) for multimedia services. The IMS authentication keys and functions at the user side are stored at the ISIM. The main architectural elements in IMS are the Session Initiation Protocol (SIP) proxies, Call Service Control Functions (CSCF) and Home Subscribe Server (HSS). CSCF consists of Proxy CSCF (P-CSCF), Interrogating CSCF (I- CSCF) and Serving-CSCF (S-CSCF). The IMS process is to receive a request from a UE, the Proxy CSCF (P-CSCF) redirects and forwards the SIP message to the I-CSCF within the UE's home network. Then, I- CSCF contacts the HSS for suitable S-CSCF to forward the registration request.

Upon the receipt of the request, the S-CSCF contacts the HSS to obtain the user's authentication data to authenticate the UE and provide the session control of the multimedia services. Once the UE has successfully established a security association with the network and a separate security association with IMS, an access will be granted to multimedia service.

These are mainly IP protocols such as SIP for user session control and Diameter for AAA (Authorization, Authentication and Accountability). Other protocols such as the Session Description Protocol (SDP) and Real time Transport Protocol (RTP) are exploited for media negotiation and transmission.

II. THE RELATED WORK

In [1], the authors introduced the proposed system which used TLS or IPSec to provide authentication, integrity and confidentiality by using securing SIP message in the lower layer attack. But they don't provide security in the higher layer attack. The feasible solution that can degrade the efficiency of previously described attacks is the deployment of Intrusion Detection System (IDS). IDS enhance the existing security with protection against unauthorized access or misuse of IMS services. All incoming and outgoing SIP messages are secured by IDS. Incoming SIP messages are passed through IDS which maintain a database of active legitimate connection. This database is updated when a new user is attacked to IMS or disconnected. Each SIP message is passed through an inspection filter to check predefined rule for attack detection. When it detects attack, the user put it in blacklist of URI of all malicious users. This schema uses Fokus open IMS core network implementation for real time and includes SIP Express Router (SER) for SIP interface and SQL database. IMS attacker creates malformed message towards IMS core by using BYE/CANCEL, malformed messages and SQL injection attack. The disadvantage of this schema is detection delay.

In [2], the authors introduced the proposal system used Intrusion Detection and Prevention (IDP) which deployed and investigated Streaming service enable (SEE) against the flooding attacks such as DoS and DDoS. SEE provide multimedia value added services. IDP detected unauthorized access or misuse of network resources in order to detect malicious messages which compared with attack rules. The performance is based on measuring the processing overhead for attacks detection. This means that it produced high performance but it is high cost.

In [3], the authors introduced the proposal system which used signature based intrusion detection system to perceive the malformed messages. After comparison with the signature, all non-complaint messages are discarded system. The authors noticed that the proposed system doesn't cover all types of malformed messages.

In [4], the authors introduced the proposal system for detecting both malformed SIP messages and SIP flooding attacks. The proposed mechanism covers three additional SIP threats. The strengths of proposed mechanism are the secure rules which displayed the improvement apparently for detecting malformed SIP messages. Second; modifying the original state transitions and utilizes a threshold based on practical VoIP services. Proposed state transition models with the threshold have not interrupted existing VoIP services, and it is possible to recognize flooding conditions. Third; through using SIP features from the rule sets and state machines, proposed mechanism catches three more SIP attacks; invalid header field, improper message transmission and session information mismatch.

In [5], the authors introduced the proposal system which present a rule based IDP. SIP headers are classified into mandatory, optional and non-allowed. It provided new rules to cover the disadvantage of RFC 3261. RFC 3261 is a request response protocol for initiating and managing communications sessions.

In [6], the authors introduced the proposal system which provided an insight about protecting the PCSCF by anomaly detection algorithm as KNN. This paper displayed high detection rate for intrusive attacks with low false positives. The proposed may be expensive because it will check each packet received.

In [7], the authors introduced the proposal system which used a self -learning component. The principle consists of retraining the anomaly detector periodically by using traffic which has been flagged as normal. The verification is comparison with last training sample. The result displayed 99% detection rate with no false positives.

In [8], the authors introduced the proposal system for disguising malformed SIP messages. They built testing system or evaluation the capability of SIP IDS on evasion rate of malformed SIP messages to prevent them from evasion.

In [9], the authors introduced the proposal system which presented attack detection schema (ADS) to provide security from SIP flooding attack. The proposed schema includes a key authentication schema for proficiently analyzing SIP packets. The proposed authentication is placed between the transport and application layers. Since the proposed schema includes a key authentication schema, the Open IMS Core analyzes SIP traffic internally to detect anomalous attacks. A network traffic tool, Ntop is configured with the Open IMS Core to analyze SIP traffic, RTP traffic and throughput rate.

In [10], the authors introduced the proposal system which presented security model to protect IMS resources or services. The proposed system presented authorization module against unauthorized access. It provided security against lower layer attack in specific domain. It provided not only authentication but also authorization.

In [11], the authors introduced the proposal system which used Genetic Intrusion detection based solution is proposed for detecting such attacks and make the services of IMS is available all time for all users. This paper explained the user cannot subscribe the IMS services without the PCSCF. But by implementing the Intrusion based detection system with some certain rules in Open IMS core environment results shows that the IMS is free from the DoS and DDoS attacks at P-CSCF point which causes the service engaged for the intended users.

III. THE IMS FRAMEWORK ARCHITECTURE

The architecture of IMS consists of four layers. Common functions and service enablers of each layer are mutualized by several applications. Functions and elements harmonization are based on the SIP protocol.

- Access Layer. The end user connects to IMS over an access network, which can be wired or wireless and includes different technologies, including Laptop, Cellular phone, xDSL, PDA, VOIP.
- Transport Layer. It is based on packet switching and consists of switches and routers which are connected over linked different technologies such as IPV4, IPV6, and CDMA. It includes mechanisms for QoS like differentiated service.

- Control Layer. This layer controls the authentication, routing, and distribution of IMS traffic between the transport layer and the service layer. The traffic is based on the SIP which provides several functions such as registration of endpoints, routing of signaling messages and overall coordination of media and signaling resources. The control functions are implemented by the most significant IMS network elements. IMS network elements (Open IMS Core) are SIP proxies, CSCF and HSS. CSCF has facilitated the correct interaction between the application servers and media servers. HSS is responsible for the centralized repository for all subscriber account information.
- Application layer. It is a set of application servers hosting different multimedia services such as Application Servers (AS) and Media Servers (MS) and Multimedia Resource Function (MRF) providing Value added services for end users. [16, 18,19]

A. *The IMS Elements*

The IMS consists of five main elements: call session control function, multimedia resource function, interworking components, application server, and databases as shown in Figure 1.

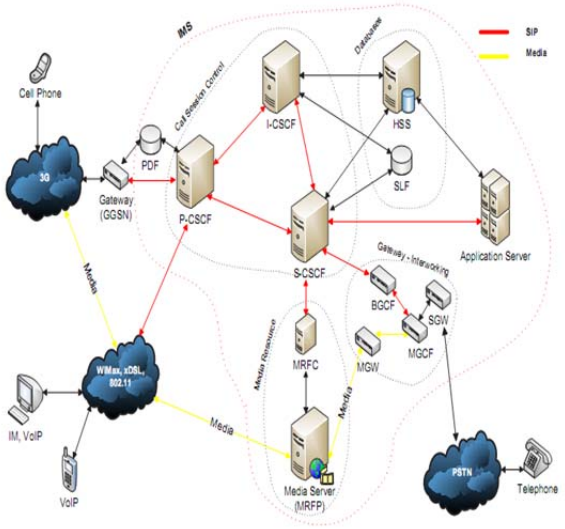

Fig. 1 The IMS Elements [16]

1) Call Session Control Function (CSCF)

The CSCF is considered the core of the IMS architecture. It is responsible for processing and routing SIP messages for the purpose of session control. CSCF functions are divided into three main categories:

1. P-CSCF is the access point to the IMS services and routes incoming requests to the appropriate network entities. It preserves security associations with the UE, executes SIP compression, and handles billing specific information. It may mix the Policy Decision Function (PDF) or can communicate with it over the diameter protocol.
2. I-CSCF communicates with the HSS over the diameter protocol in order to assign S-CSCF for the registration of UE. It provides the access to the home domain when the user is visiting other networks. It provides Topology Hiding Inter Network Gateway (THIG) functionality through the encryption of "Record-route" and "Via" headers.
3. S-CSCF is a SIP server and acts as registrar during the registration procedures. It is responsible for the session handling and for the retrieval of the authentication vectors and user profiles from the HSS. In multi-HSS environments, it communicates with the Subscription Locator Function (SLF) to locate the HSS that holds the data of a specific user. It forwards the SIP messages to the Breakout Gateway Control Function (BGCF) to communicate with the PSTN network.

2) Multimedia Resources Function (MRF)

This element handles the media services such as conferencing sessions, audio and video transcoding. It consists of two subcomponents:

1) Media Resource Function Processor (MRFP) mixes the media streams and provides media sourcing.

2) Media Resource Functions Controller (MRFC) controls media resources in the MRFP and it is responsible for interpreting the incoming traffic and signaling from an S-CSCF or an AS.

3) Interworking element

It performs media and signaling conversion between circuit switched or mobile and IP networks. For routing a request, signaling data are forwarded *through* BGCF, which accepts the SIP signaling from the S-CSCF and determines the next hop in the PSTN. It locates an appropriate Media Gateway Control Function (MGCF), which is responsible for mapping different signaling protocols between the IMS and the PSTN network. The Media Gateway (MGW) converts and transcodes the media exchanged between the IMS and circuit switched network entities. The Signaling Gateway (SGW) provides bidirectional signaling conversion between the IP and SS7 transport protocols.

4) Application Server (AS)

It provides the IP multimedia services to the home network or to other locations. It can also provide OSA (Open Service Access) services in the IMS and it acts as a gateway to legacy service networks such as Customized Applications for Mobile Network Enhanced Logic (CAMEL) through the deployment of corresponding servers. The AS uses the diameter protocol to communicate with the HSS or the SIP with S-CSCF and it may also interface with the MRFC for media control. [16, 18, 27]

5) Databases

The HSS is the main warehouse of IMS subscriber's data. It holds users' profiles, location, security and any other information required for the service provision. HSS is contacted by other network elements (S-CSCF or I-CSCF) whenever an incoming request requires authentication or authorization according to the provider's policy by using the Diameter protocol.

IV. THE IMS FRAMEWORK SECURITY

In order to access the multimedia services, LTE users have to be authenticated in both the LTE network layer and the IMS service layer. An IMS subscriber needs the mutual authentication with the LTE network by the Extensible Authentication Protocol- Authentication and Key Agreement (EPS-AKA) before the access to multimedia services. An IMS AKA is executed between the ISIM and the Home Network (HN) for IMS AKA. 3GPP specifications deliver guidelines to ensure access and network domain security.

A. Access and Network Domain Security

1) Access security
   - SIP signaling protection between the subscriber and IMS uses IPsec for data confidentiality, integrity and origin authenticity.
   - Mutual authentication between subscribers and IMS uses AKA.
2) Network domain security is enforced by using security gateways, topology hiding techniques and IPsec for data encryption or integrity verification.

B. The IMS Architecture Security

IMS Architecture Security is divided into five different security Associations as shown in Figure 2.

1) The association between UE and IMS Core:
   The authentication process is done by HSS which is responsible for generating the keys used in this process.
2) The association between UE and P-CSCF:
   It provides authentication of data origin and builds a secure link between the UE and P-CSCF.
3) The association between CSCF and HSS:
   This association plays an important role in securing the keys during the UE registration process and it provides internal security for the link between a CSCF and HSS. This is known as the Cx interface. All interactions on Cx happen using the Diameter protocol to provide a reliable transport and overcrowding control which based on TCP and SCTP. The Diameter protocol provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility in both local and roaming situations.
4) The association between P-CSCF and other SIP core services:
   It provides security between a P-CSCF and other SIP core when the UE is roaming to a Visited Network (VN). This specifies the use of IPSec on this interface and the use of IKE (internet key exchange) for negotiation of security agreements between the CSCFs. The Za interface is used between the differences of security domains and is protected by using these mechanisms.
5) The association between P-CSCF and other core SIP:
   It provides security between the P-CSCF and other core SIP services when the UE is operating in the HN.

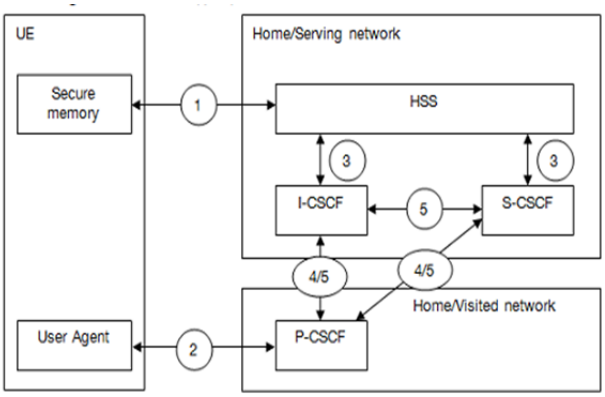

Fig. 2 The IMS Architecture Security

C. The IMS Security Mechanisms

The capabilities of IMS security mechanisms against attacks occur during session and registration procedures. An attacker can be either an External Attacker or an Internal Attacker. An External Attacker (EA) launches attacks against the IMS infrastructure without having authorization to access the network. An Internal Attacker (IA) is a legitimate user and thus authorized to access network services. An internal attacker establishes security tunnels with the proxies, authenticate malicious packets, and gather important information to launch attacks.

In IMS architectures, authentication takes place during the registration procedure. The main authentication schemes are: SIP Digest, IMS AKA with the IPsec, and TLS with SIP Digest. TLS and IMS AKA offer confidentiality and integrity capabilities.

SIP Digest, An attacker initiates during the registration procedure since the first unprotected message is sent. An IA could be a subscriber who tries to overload with calls and cause denial of service (DoS) to a person in her contact list. An EA could be a passive eavesdropper who tries to obtain a legitimate user's password by monitoring the communication with the server.

The TLS with SIP Digest, the authentication procedure is the same way as in the SIP digest. But the main difference between SIP Digest and TLA with SIP Digest is that the second REGISTER message of TLS authentication scheme is protected through the integrity and confidentiality mechanisms which are provided by the specific protocol.

The IMS AKA is considered as the strongest authentication scheme that can be deployed in cases where a UE embeds an ISIM. This scheme is similar to the SIP digest, but IMS AKA establishes a secure tunnel between the UE and P-CSCF which provides integrity and confidentiality. It protects communication messages against attacks such as the Man-in-the-Middle (MIM), eavesdropping and all subsequent messages are protected through the same security tunnel.

V. THE IMS LAYER THREATS

IMS network elements (Open IMS Core) have been exposed to many attacks. The attacks ways are Flooding attack and Anomalous SIP request. In flooding attack, an attacker sends numerous SIP related request messages to a user, which overloads the SIP server or Open IMS Core. It

leads to end the session and an unexpected session loss degrades network performance of the Open IMS Core. In the Anomalous SIP request, an attacker sends an anomalous SIP request to confuse the Open IMS Core or to collect the server to execute the anomalous code. The Attacks in the IMS can be classified into time-dependent and time-independent attacks. The time-dependent attack means that a time interval is required to damage the victim such as flooding attack. Time-independent attack means that its effect is immediately on the target as a data packet arrives such as SQL injection attack.

A. Application layer threats

The application may contain malicious contents (viruses or worms). The intruders can easily distribute botnet clients on users' terminal to perform attacks such as DDoS, eavesdropping, spam distribution, and fraud. This problem is even more critical when the operators act as providers of third-party application contents.

ASes are networked entities with which value added services are hosted. ASes can be placed either in the operator's home network or in a third party network. This makes IMS services more vulnerable because operators cannot totally control third party activities. ASes can also communicate with each other or with the existing Internet services, so user data is shared over this communication. Once an intruder gains access to one application, he/she might be able to eavesdrop or alter information coming/going from/to other applications.

B. Control layer threats

Control layer threats activities consist of sending and treating SIP signaling messages between IMS elements, so a normal functioning of this layer depends on the correctness and security of SIP messages. SIP suffers from a lot of vulnerabilities including:

1) SIP flooding attacks such as Invite, Register, Invite Response, Register Response and Options flooding attacks.
2) SIP parser attacks such as malformed messages and sequence disorder attacks.
3) Session tearing down threats such as SIP Bye and Cancel attacks.
4) Session modification attacks such as SIP Re Invite and Update attacks.
5) Redirection attacks such as 3xx response attacks
6) REFER attacks.
7)

C. Transport layer threats

Flooding attacks such as TCP SYN and UDP flooding are the most known and widespread threats in the transport layer. Over billing attacks are also possible if the attacker can hijack the session after user disconnection.

D. Access layer threats

This layer encompasses various types of access networks including GPRS, UMTS, Wi-Fi, and xDSL.

VI. THE FRAMEWORK FUNCTIONALITIES

The Figure 3 explains our framework will apply to the incoming SIP request from UE to P-CSCF or from UE to NAF

When UE wants to send SIP request to IMS network, it must be detected before it sends. The SIP request may be infected and will be a malicious request or an error message. This framework will introduce a new IDP mechanism to monitor, detect and prevent SIP message. There is an associated IDS to detect and analyze malicious request. The IDS uses anomaly detection filtering algorithm of to filter the packets. If the message is attacked, The IDS catches and analyzes the messages. The IPS modifies and clears the packet it and later it is sent to the user (by changing the content of malicious packet). IDS notify this action. IDP detects malicious packet to be rejected and put it in black list.

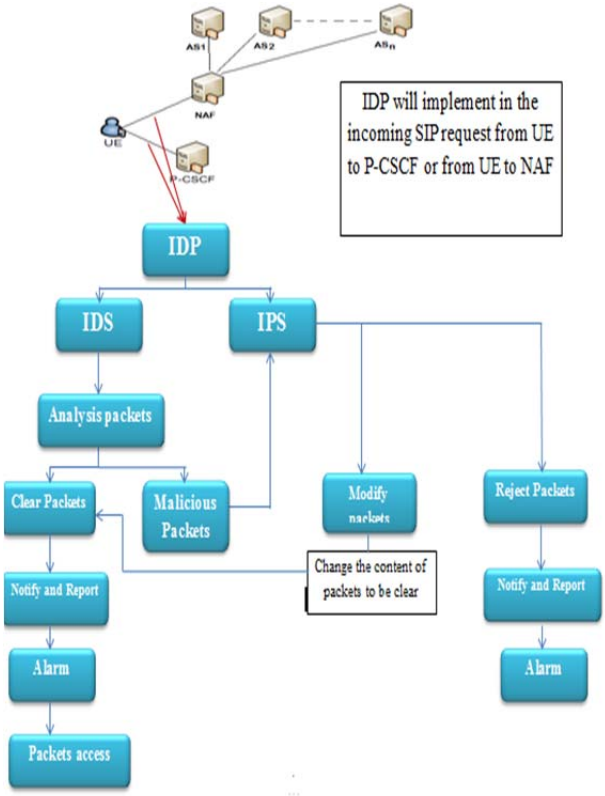

Fig. 3 The Framework Functionality Scenario 1.

Figure 4 shows the Framework Functionality Scenario 2. When UE wants to send SIP request to SEG, it must be detected before it sends in order to build a secure tunnel. SIP request from UE in The SIP request may be infected or malicious request or an error message. This framework will introduce a new IDP mechanism to secure traffic within the security domain. IDS monitor the traffic and detect malicious attack and IDP prevents attack traffic and clears it. The output of IDS is alarming and the result stored in a database or blacklist.

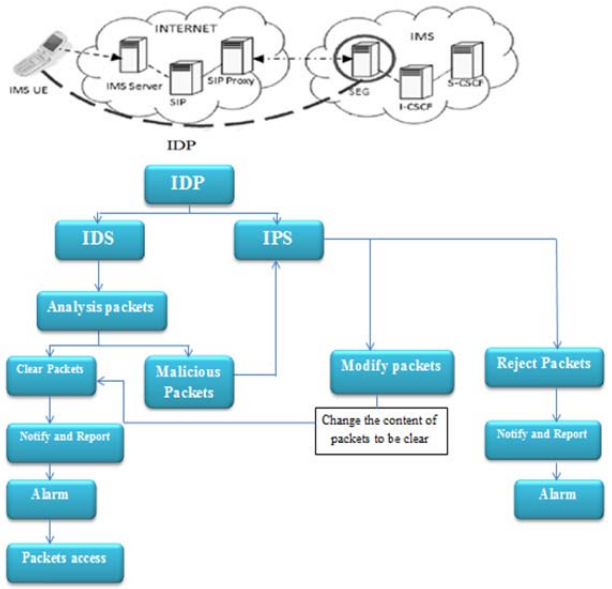

Fig. 4 The Framework Functionality Scenario 2.

VII. CONCLUSIONS

This paper proposed an IP Multimedia Framework for LTE networks with multimedia services is proposed. The proposed framework has advantages such as easy development and deployment of new services, high level of quality of service, and common billing and charging functionalities. It is based on IP protocols which provide the best effort service. The paper creates an architecture for deploying VoIP applications that provides for both QoS and charging, and for efficiently integrating multiple different services, which can be easily mixed and matched to meet the user needs. The paper analyzes IMS layers vulnerabilities and then presents two scenarios to handle such attacks. The proposed system has contributions; comprehensive design to authenticate the SIP message and new scalable design of using IDP to monitor, detect and prevent SIP message attacks. First scenario provides new authentication algorithm between UE and open IMS core (P-CSCF) to authenticate the SIP message. The framework uses IDP to monitor, detect and prevent SIP message attacks. Second scenario creates authentication between the P-CSCF and other SIP core in HN (secure component within the security domain). IDS monitor the traffic and detect malicious attack and IDP prevents attack traffic and clears it. In order to access the multimedia services, the framework allows the users to be authenticated in both the network layer and the IMS service layer. In this framework, the subscriber needs the mutual authentication with the network by the EPS-AKA before the access to multimedia services.

REFERENCES

[1] Michail Tsagkaropoulos, Ilias Politis, Tasos Dagiuklas and Stavros Kotsopoulos, “Securing IP multimedia subsystem (IMS) infrastructures: protection against attacks”, Proceedings of FITCE Congress 2008, Session 07: Paper 05, 2008.

[2] Peeyush Mathur, Bharat Singh, Raj Kumar Sain and Chandra Shekhar, “Next generation networks: Enhancing Performance and Security for providing Mobile Multimedia Broadcasting”, Proceeding. 4th National (India), 2010.

[3] Geneiatakis et al., “A framework for protecting a SIP-based infrastructure against malformed message attacks”, Computer Networks, vol. 51, no. 10, July 2007, pp. 2580–2593.

[4] D. Seo, H. Lee and E. Nuwere, “Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models”, 23rd IFIP TC11 Int. Information Security Conference (SEC), Milan, Italy, September 2008, pp. 397–411.

[5] H. Li et al. “A rules-based intrusion detection and prevention framework against SIP malformed messages attacks”, 3rd IEEE Int. Conf. on Broadband Network and Multimedia Technology (IC-BNMT), Beijing, China, October 2010, pp. 700-705.

[6] A.H. Farooqi and A. Munir, "Intrusion Detection System for IP Multimedia Subsystem using K-Nearest Neighbor Classifier", IEEE Int. Multitopic Conference (INMIC), Karachi, Pakistan, December 2008, pp. 413-428.

[7] K. Rieck et al., “A self-learning system for detection of anomalous sip messages”, Principles, Systems and Applications of IP Telecommunications - Services and Security for Next Generation Networks (H. Schulzrinne et al., Eds.), LNCS 5310, Springer, 2008, pp. 90–106.

[8] Yulong Wang and Lei Wang, “A Method for Disguising Malformed SIP Messages to Evade SIP IDS”, Journal of software, Vol. 8, no. 11, 2013, pp. 2830-2838.

[9] Bakkiam David Deebak, Rajappa Muthaiah, Karuppusamy Thenmozhi and Pitchai Iyer Swaminathan, “IP Multimedia Subsystem - An Intrusion Detection System”, Smart Computing Review, vol. 3, no. 1, February 2013.

[10] Qasim Jan and Shahzad Latif, “IP Multimedia Subsystem (IMS) security model”, International Journal of Advance Research, IJOAR .org , vol. 1, Issue 3, March 2013, pp. 1-6.

[11] Muhammad Tayyab, Ahmed Mateen Buttar, Milhan Afzal Khan and Muhammad Awais, “TO Overcome DoS and DDoS Flooding Attacks in IP Multimedia Subsystem (NGN) using the Genetic Intrusion Detection Systems (IDS)”, International journal of scientific & engineering research, volume 4, issue 1, january-2013.

[12] Haitao Meng, “A Preliminary Research on Security Issues in IP Multimedia Subsystem”, IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012), Sichuan, 29-31 May 2012, pp. 2560 – 2564.

[13] Elmostaf A Belmekki, Brahim Raouyane, Abdelhamid Belmekki and Mostafa Bellafkih, “Secure SIP Signalling Service in IMS network”, IEEE Intelligent Systems: Theories and Applications (SITA-14), 2014 9th International Conference on, Rabat,7-8 May 2014, pp. 1-7.

[14] Hamid Allouch and Mostafa Belkasmi, “Design of distributed IMS by classification and evaluation of costs for secured architecture”, IEEE Innovative Computing Technology (INTECH), 2012 Second International Conference on, Casablanca, 18-20 Sept. 2012, , pp. 291 – 296.

[15] E.Belmekki and M.Bellafkih, “Efficient light model for securing IMS network”, IEEE Intelligent Systems: Theories and Applications (SITA), 2013 8th International Conference on, Rabat, 8-9 May 2013, pp. 1 – 7.

[16] Nikos Vrakas, Dimitris Geneiatakis, and Costas Lambrinoudakis, “Evaluating the Security and Privacy Protection Level of IP Multimedia Subsystem Environments”, IEEE communications surveys & tutorials, vol. 15, no. 2, second quarter 2013, pp. 803-819.

[17] Shih-Yuan Cheng and Whai-En Chen, “A Fast SA Update Mechanism for Secure SIP/IMS Mobility in Integrated UMTS-WLAN Networks”, IEEE 2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, Taichung, 3-5 July 2013, pp. 281 – 286.

[18] Somia NATOURI and Chidung LAC, “IMS Threats Taxonomy: Survey and Proposal”, IEEE Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, Ho Chi Minh City, Vietnam, 21-24 Jan. 2013, pp. 315 – 320.

[19] Somia Natouri, Chidung Lac and Ahmed Serhrouchni, “A Model-Based Resilience Analysis for IMS”, journal of network, vol. 9, no. 3, march 2014.

[20] Frank S. Park, Devdutt Patnaik, Chaitrali Amrutkar and Michael T. Hunter, “A Security Evaluation of IMS Deployments”, IEEE Internet Multimedia Services Architecture and Applications, 2008. IMSAA 2008. 2nd International Conference on, Bangalore, 10-12 Dec. 2008, pp. 1 – 6.

[21] Do van Thanh, Paal Engelstad and Do van Thuan, "Authentication in a multi-access IMS environment", IEEE Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing, Avignon, 12-14 Oct. 2008, pp. 613 – 618.

[22] Kai-Di Chang, Chi-Yuan Chen, Jiann-Liang Chen and Han-Chieh Chao, "Challenges to Next Generation Services in IP Multimedia Subsystem", journal of Information Processing Systems, Vol.6, No.2, June 2010.

[23] Hamid Allouch and Mostafa Belkasmi "Design of Transparent Distributed IMS Network: Security Challenges Risk and Signaling Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.4, No.4, December 2012.

[24] E.Belmekki, N.Bouaouda, B.Raouyane and M.Bellafkih, "IP Multimedia Subsystem: security evaluation", Journal of Theoretical and Applied Information Technology 10th, May 2013, Vol. 51 No.1.

[25] Muhammad Sher and Thomas Magedanz, "Mobile Multimedia Broadcasting Vulnerability Threats, Attacks and Security Solutions", 9th International Conference on Mobile and Wireless Communications Networks, Cork. Ireland, September 19-21. 2007, pp. 56 – 60.

[26] Salekul Islam and Jean-Charles Grégoire, "Multi-domain authentication for IMS services", Elsevier journal, Computer Networks 55 (2011), pp. 2689–2704.

[27] Gonzalo Camarillo, and Miguel A. Garc´ ıa-Mart´ ın "The 3G IP Multimedia Subsystem (IMS) - Merging the Internet and the Cellular Worlds", Wiley, Second Edition, 2006.

[28] Salekul Islam and Jean-Charles Grégoire, "Multi-domain authentication for IMS services", Elsevier journal, computer networks 55 (2011), pp. 2689-2704

.