STRENGTHENING SECURITY OF IP MULTIMEDIA SUBSYSTEM

Nauris Paulins
Latvia University of agriculture
nauris.paulins@llu.lv

Abstract. IP Multimedia Subsystem (IMS) is defined by 3GPP/3GPP2 and has become as a major part of the next-generation networks (NGN) service delivery platform. IMS provides convergence of two most successful communication paradigms – data networks (the Internet) and cellular networks on IP based infrastructure. Such platform allows an easy development of new value added and multimedia services. Open architecture of IMS brings big challenges in privacy and security. The 3GPP standards already specify such security solutions like authentication, key agreement and Transport Layer Security (TLS), but IMS is still vulnerable to several attacks in their services, like VoIP or multimedia conferences. There is still a risk to flooding attacks, DoS and DDoS attacks, because IMS used protocols (Session Initiation Protocol, Diameter Protocol, Media Streaming and Internet protocol) are fully opened and can be easy accessed from intruders. This paper focuses on a possibility to minimize the potential risks of IMS, by integrating intrusion detection and prevention system (IDS/IPS). The experimental tests are performed on OpenIMS Core on different type of flooding, spoofing and DoS attacks.

Keywords: IP multimedia subsystem, security, intrusion detection and prevention.

Introduction

Communication networks have become a key infrastructure for many areas. It plays an important role in rural engineering as well. The possibilities that bring the Internet and mobile phones increased importance of communication networks. However, the requirements for data speed, mobility and new services are growing all the time. This is the reason why the idea about convergence of telecommunication networks and data networks becomes more and more popular [1]. Network convergence is driven by the shift towards IP-based broadband networks. It includes fixed-mobile convergence and ‘three-screen convergence’ (mobile, TV and computer).

To provide multiple services with multimedia requires management of the Quality of Service (QoS). This means being able to manage user sessions, assign new facilities and provide security for service delivery. IP multimedia subsystem (IMS) was specially developed for network convergence and session control; it brings what the traditional IP networks could not support.

To deploy correctly functional and effective IMS architecture in the area of service delivery a well-structured and fully functional security framework should be applied. The foremost attribute of IMS is the notion that all infrastructures will be moved onto an Internet Protocol platform. Such openness for telephony networks is something new. Telephone communications are characterized by carefully guarded endpoints. Both endpoints must be recognized by the other carrier, which is done with telephone numbers. All process is carefully controlled and available only for authorized parties. Moving to Internet protocols means openness and vulnerabilities. Vulnerabilities of IP networks make IMS a popular target for hackers or intruders. Different types of attacks can be generated by intruders to destroy the performance of IMS, causing denial of service (DoS). It can be done with attacks like REGISTER flooding attacks or INVITE flooding attacks, which are overloading the IMS core computational resources. The current security frameworks do not protect IMS against such attacks.

Most of the previous work on IMS security has focused either on preventive measures or on response to the known threats. The aim of this research is to protect the IMS core components like P-I-S-CSCF, HSS from DoS attacks like SIP flooding, BYE attacks, SIP Register flooding, SIP INVITE flooding, by monitoring system load and making adaptive traffic control to prevent the system overload from DoS attacks. This is a flexible mechanism which can assign the users by priority or subscription in critical load study.

Materials and methods

IMS architecture is divided into three layers: the user layer, session control layer, and application layer as it is shown in Fig. 1. The user layer provides for termination of signaling to end points, routing and control of bearer traffic. The session control layer handles the registration of endpoints and routing of SIP messages to the appropriate application servers. The application layer comprises application servers which provide IMS customers with services such as Presence, Instant message, and Push to talk [2].

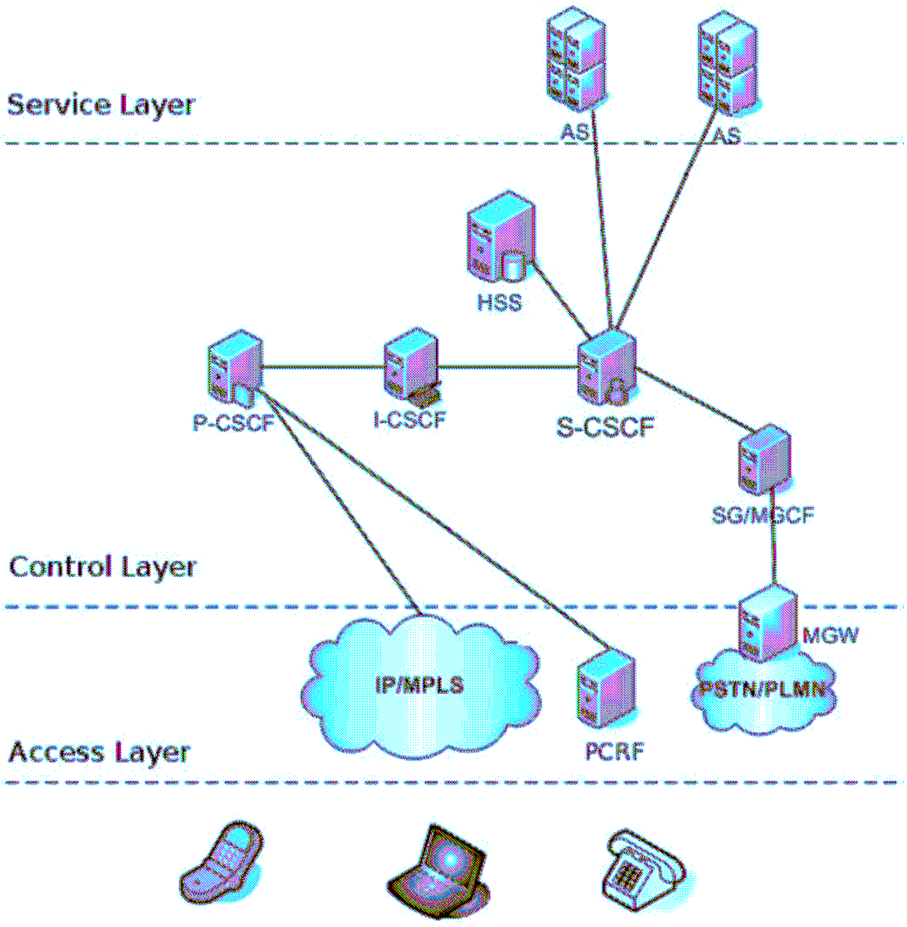

Fig. 1. **IMS Architecture**

The main components of the IMS core are CSCFs (Call Session Control Functions), MGW (Media Gateway), HSS (Home Subscriber Server) and other components. Proxy CSCF (P-CSCF) is the first contact point for SIP compatible devices to IMS. The interrogating CSCF (I-CSCF) provides entrance to the home domain and assigns S-CSCF. The serving CSCF (S-CSCF) is doing registration of endpoints, user authentication, service control.

Distribution of the IMS core component functions to different entities in an IP network provides a greater number of opportunities for an attacker to intrude the IMS core components. The IMS already has its security framework which is divided into two parts: access security and network security. Access security includes authentication related mechanisms and traffic protection between the user equipment (UE) and core network, this part is specified in 3GPP TS 33.203 [3] specification. Network protection includes traffic protection between the network elements and also roaming and non-roaming scenarios, which is specified in 3GPP TS 33.210 [4] specification.

But IMS is still vulnerable to several types of attacks like DoS and DDoS attacks. These attacks are a large number of random messages sent from single or multiple malicious nodes to overload network resources. The attacker can lunch a huge amount of messages, up to 10 000 messages per second, which is equivalent to the traffic from 10 million subscribers [5]. Attacks on IMS core can be categorized by time dependent and time independent attacks [6]. Time dependent attacks aim to exhaust resources at different levels, from the link bandwidth to the computational resources. Most dangerous for IMS core are flooding attacks like TCP/SYN flooding, Smurf attacks, REGISTER flooding attacks, INVITE flooding attacks, INVITE and REGISTER response attacks. Analysis of IMS vulnerabilities was made in [7], where vulnerabilities were discovered, which is shown in

Table 1. On the basis of this analysis a security mechanism against the existing flooding attacks has been proposed, because these are ones of the most dangerous attacks in service delivery.

Table 1

IMS vulnerability list [7]

Vulnerability	Weakness	Security dimension	Asset module	Impact
Message spoofing	IMS has absence of IPsec protection between user equipment and P-CSCF	Authentication	Service layer Control plane	Fraud of trust
SIP SQL injection	SIP authentication controllability is unsecure	Availability	Service layer User plane	Deniel of service
Media theft	Not enough control on media streems	Non-repudiation	Infrastructure layer Management plane	Theft of sercices
SIP flooding	Unable effectively prevent REGISTER and INVITE message flooding	Availability	Infrastructure layer Control plane	Loss of QoS for users
RTP data sniffing	No default confidentiality from data streem	Confidentiality	Application layer User plane	Theft of information
CANCEL attack	Possibility to fake SIP CANCEL request	Integrity	Service layer Control plane	Session disruption
RTP injection	RTP protocol missing media integrity protection mechanisms	Integrity	Service layer User plane	Session disruption
Man in the Middle P-CSCF attack	Authentication using SIP must be improved	Authentication	Service Layer Control plane	Impersonation of a server
Dictionary attack	Inadequate identity protection and AKA chipper algorithm use	Authentication	Application layer Control plane	Identity theft
BYE attack	Possibility to fake SIP BYE request/ not enough confidentiality protection	Integrity	Service layer Control plane	Disruption of session
DNS Cache Poisoning	Not enough connection integrity protection	Integrity	Infrastructure plane Control plane	Loss of service
Network topology disclosure	Not protected SIP messages	Confidentiality	Infrastructure layer Control plane	Leak of network topology
HTTP Parse Attack	Improperly data ContentLenght regulation	Availability	Infrastructure layer Control plane	Loss of services
User equipment configuration tampering	Probability lack of user education in security questions	Availability	Infrastructure layer Control plane	Denial of services

The proposed security mechanism focuses on protecting the IMS core components – CSCF functions, implementing Intrusion Detection and Prevention System (IDS/IPS). In this paper Hellinger Distance has been proposed as an anomaly detection method. Hellinger distance (HD) quantifies the deviation between two probability measures. In [8] HD it has been used to detect SIP message anomalies. Attributes from SIP messages were INVITE, 200 OK, ACK and BYE packets arrived in a predefined time-window. The algorithm consists of the training phase and testing phase. If observed HD is greater than the threshold value then alarm is raised. The proposed security mechanism was tested on OpenIMS core designed by the Fraunhofer Institute Fokus in Berlin. It aims to establish experimental environment for developers and designers to have a chance to create, modify and study IMS services. Basic IMS architecture is shown in Fig. 2.

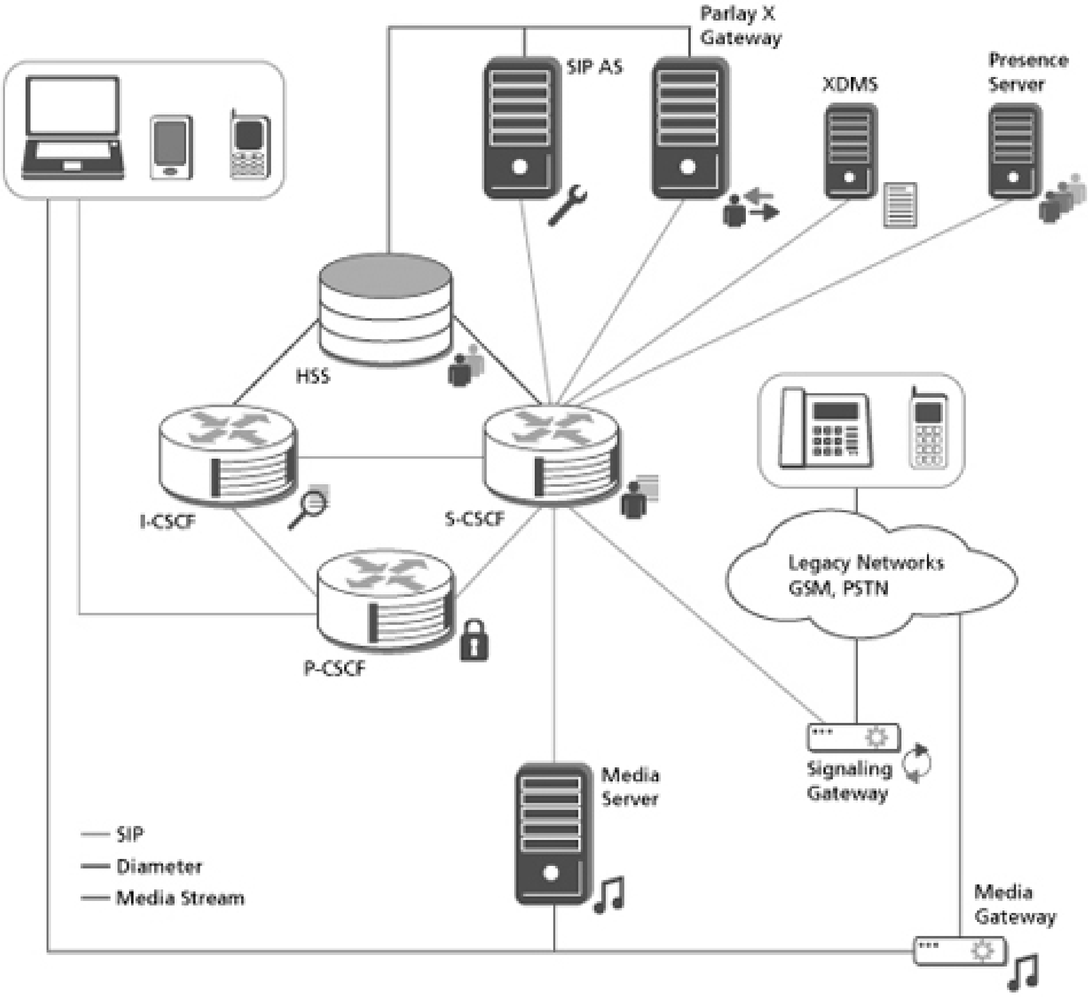

Fig. 2. **OpenIMS Architecture**

Whenever the User Equipment (UE) wants to start communication with OpenIMS Core, it has to register with IMS. The OpenIMS Core is downloaded and installed on Intel Core2Duo E7300, 2.66 GHz and 2 GB RAM on Ubuntu operation system. P-CSCF is the first entry point that is why the packets received at P-CSCF will go through anomaly inspection. There was attack traffic injected to generate the data set for testing. XML language was utilized to build attack scenarios. The call rate in SIP is fixed at 60 seconds and traffic was generated using SIPp tool, which is a free Open Source test tool / traffic generator for the SIP protocol [9]. For the training phase a scenario was created with varying traffic load on P-CSCF and for the testing phase also a scenario was created with different attack intensity varying from 25 calls·s^{-1} – 50 calls·s^{-1}. For the training phase a scenario was created with normal traffic 500 calls·min^{-1}. For each dataset the number of INVITE, ACK, 200 OK and BYE packets was calculated. There was the threshold value according [8] and if sip messages cross this threshold than alarm is notified. Also the algorithm detection rate and false alarms were calculated. For traffic analysis Wireshark software was used, which is a protocol analyzer with the ability to capture and interactively browse traffic running on the computer network [10].

Results and discussion

The anomaly detection module is analyzing incoming traffic in P-CSCF. On normal traffic load SIP Flooder was created, which floods REGISTER messages. Normal data load on the training phase is shown in Figure 3, but Figure 4 shows how the flooding attacks reduce the processing performance of P-CSCF server and rising denial of services for users. It can be seen that on the attack intensity 25 calls·s^{-1} there is some communication intensity, but on 50 calls·s^{-1} it is falling totally down.

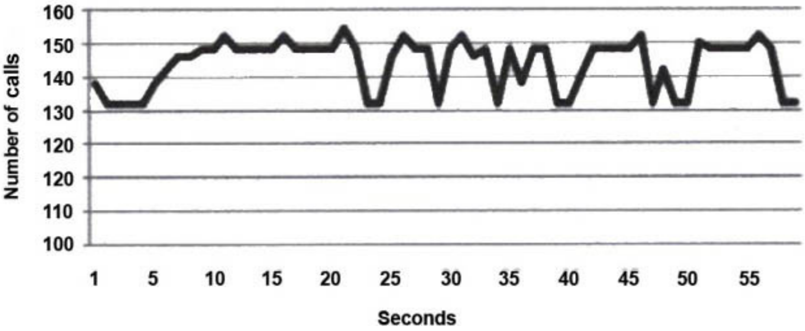

Fig. 3. **Calls processing on normal traffic load**

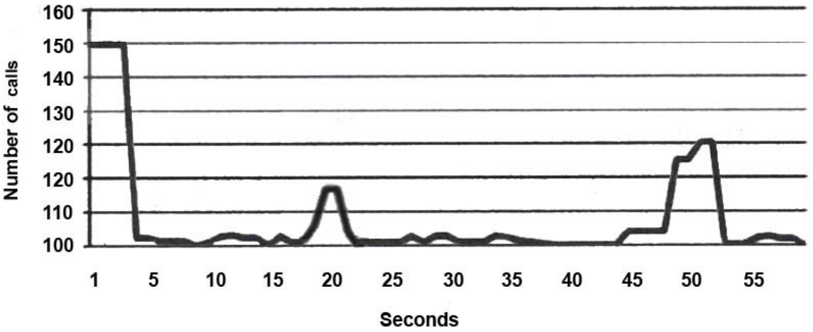

Fig. 4. **Calls processing on flooding attack load**

The Hellinger distance has shown low false alarm rate, it was about 2 %. Such result gives an idea to extend the effectiveness testing on various attack types. Using the Hellinger distance for P-CSCF protection normal calls processing could be provided like inf Figure 3 and OpenIMS have shown good processing recovery. The overall detection rate 98 % has shown that this method is a robust and effective detection method for protecting against flooding attacks. This is an anomaly detection algorithm which could be tested together with some signature-based protection, which would allow providing hybrid protection for IMS core functions.

Conclusions

IP multimedia Subsystem is implemented on top of IP and SIP protocols. It is important to protect the IMS core elements from intruders, especially P-CSCF as the first entry point for user devices. IP multimedia subsystem is still vulnerable to several attacks, which must be prevented. In this paper the Hellinger distance algorithm as an anomaly detection method was tested, there was the detection accuracy tested for malicious traffic for P-CSCF protection. The Hellinger distance algorithm has shown good accuracy in anomaly detection with a low false positive rate. Currently this approach can be quite expensive as it checks each packet; some performance optimization could be done in future. The IMS performance and security analysis can be further designed to extension for the existing specifications. The open source IMS platform allows performing IMS testing to validate and refine various security models.

Acknowledgements

This research has been supported by the European Social Fund within project "Support for the Implementation of Doctoral Studies at Latvia University of Agriculture", /2009/0180/1DP/1.1.2.1/09/IPIA/VIAA/017.

References

1. Salina J. L., Salina P. Next Generation Networks, Perspectives and Potentials, John Wiley&Sons Ltd, 2007. 254 p.
2. Shuang K.S., Zhang B., Su S. IMS Security Analysis using Multi-attribute Model, Journal of Networks, vol. 6, 2011, pp. 263 – 271.
3. 3 GPP TS 33.203: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP based services (Release 7).
4. 3GPP TS 33.210: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Network Domain Security; IP network layer security (Release 7).
5. Awais A., Farooq M., Javed M.Y. Attack Analysis and Bio-Inspired Security Framework for IP Multimedia Subsystem Categories and Subject Descriptors. Defense Journal, 2010, pp. 161-162.
6. Sher M., Wu S., Magedanz T. Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS), 2006, pp. 38 – 44.
7. Paulins N., Rivza P. Vulnerability Analysis of IP Multimedia Subsystem (IMS), Proceedings of the 5-th International Scientific Conference Applied Information and Communication Technologies, 2012, pp. 104 – 113.
8. Sengar H., Wang H., Wijesekera D., Jajodia S. Detecting VoIP Floods using Hellinger Distance, IEEE Transactions on Parallel and Distributed Systems, vol. 19, 2008, pp. 794 – 805.
9. SIPp Open Source SIP protocol trafic generator. [online] [02.03.2012]. Available at: http://sipp.sourceforge.net/.
10. Wireshark network protocol analyzer. [online] [27.02.2012]. Available at: http://www.wireshark.org.