IS IP MULTIMEDIA SUBSYSTEM AFFECTED BY 'MALFORMED MESSAGE' ATTACKS?
An Evaluation of OpenIMS

Nikos Vrakas[1], Dimitris Geneiatakis[2] and Costas Lambrinoudakis[1]
[1] *Department of Digital Systems, University of Piraeus, 150 Androutsou St., Piraeus 18532, Greece*

[2] *Department of Computer Science, Columbia University*
1214 Amsterdam Avenue, M.C. 0401, New York, 10027-7003, U.S.A.

Keywords: IP Multimedia Subsystem, Session Initiation Protocol, Malformed message attacks, Security.

Abstract: In this paper we assess the open IP Multimedia Subsystem (IMS) robustness against malformed message attacks. We employ an IMS test-bed architecture using two different testing suites; the PROTOS which is publicly available, and a proprietary one, that has been develop for the purpose of this specific work. Results have highlighted that although IMS can effectively handle well-known malformed messages, such as those utilized in PROTOS, it cannot manage satisfactorily unknown malformed messages. During the attack scenarios memory consumption increases up to 25%, while the end-to-end delay experienced by the users increases up to 4000%.

1 INTRODUCTION

IP Multimedia Subsystem (IMS) (3GPP 2008) is the core of Next Generation Networks (NGNs) for delivering services in wirelline and wireless end users, under the umbrella of IP network infrastructure. IMS specifications specify and standardize the appropriate mechanisms for guaranteeing Quality of Service (QoS), security, availability and reliability of the provided services. IMS is employed on existing IP network infrastructures utilizing the Session Initiation Protocol (SIP) (Rosenberg et al. 2002) for multimedia session management.

This fact exposes IMS to existing internet threats (D. Geneiatakis et al., 2006), (Keromytis, 2010) such as resource consumption, man in the middle attacks, unauthorized session modification, and malformed message attacks. In the latter case, malicious users craft particular messages in order to affect service availability or to gain unauthorized access. Previous works (Wieser and Laakso, 2003), (Dimitris Geneiatakis et al., 2007), pinpoint poor implementations in the very early SIP based employments. Particularly, PROTOS (Wieser and Laakso, 2003) assess various SIP implementations as far as their robustness against malformed message attacks is concerned. Results have demonstrated that the examined SIP developments could not process properly and finally discard the malformed messages.

Though various solutions (Dimitris Geneiatakis et al., 2007), (Niccolini et al., 2006) have been proposed to protect SIP based infrastructures against this type of attacks and improvements have been accomplished in implementations, malformed messages are still a potential attack method against IP multimedia services. Asterisk PBX (www.asterisk.org), for example, has been found vulnerable to various malformed message attacks (e.g OSVBD 2007), giving malicious users chances to gain unauthorized access.

Under this context and taking into consideration the fact that IMS is a critical component for NGNs' proper operation, in this paper we examine the impact of malformed message attacks against the IMS architecture. To the best of our knowledge there is no published work in the literature for evaluating the side effects, in terms of users "experiences" and server side consequences, of malformed message attacks against IMS. We evaluate the open source IMS platform (Open IMS - www.openims.org), conducting different malformed message attack scenarios based on the PROTOS test

Vrakas N., Geneiatakis D. and Lambrinoudakis C..
IS IP MULTIMEDIA SUBSYSTEM AFFECTED BY 'MALFORMED MESSAGE' ATTACKS? - An Evaluation of OpenIMS.
DOI: 10.5220/0003519602750280
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 275-280
ISBN: 978-989-8425-71-3

suite. Furthermore we have developed our own specific malformed message attack tool. We measure the overhead, during an attack, in terms of the introduced latency for the users. Moreover, we assess the memory consumption on the server side. Test results confirm that the open IMS platform is robust against attacks launched through the PROTOS testing suite, while it is not for attacks launched through the developed tool. The end-to-end delay increases in a range between 300% and 4000%, while there is additional memory consumption of approximately 25%.

The rest of the paper is structured as follows. In Section 2 we present background information with regard to IMS architecture, and malformed message attacks. In Section 3 we evaluate the robustness of Open IMS system against malformed message attacks and we discuss the evaluation results. Finally, in Section 4 we conclude the paper providing some pointers for future work.

2 BACKGROUND

2.1 IP Multimedia Subsystem

The core of IMS architecture according to (3GPP 2008) consists of the following network elements:

- Proxy Call Session Control Function (CSCF) (P-CSCF) that handles and routes all signaling information (requests and responses) to the appropriate network element for additional processing depending on the type of signaling information and the kind of the service.
- Interrogating CSCF (I-CSCF) ensures communication with users' home network, acting as a proxy at the edge of the service provider network. It communicates with the Home Subscriber Server (HSS), over the diameter protocol in order to assign a Serving CSCF responsible to serve the corresponding UE.
- Serving CSCF (S-CSCF) manages (statefully) multimedia sessions and handles users' authentication: It contacts the HSS to retrieve the authentication vectors and user profiles.
- Home Subscriber Server administers users' profile, location, security and any additional information required for the service provision.

Considering that IMS network elements are logical entities they can be deployed under the same physical network element. The communication amongst IMS network elements is based on SIP. Figure 1 illustrates a high level IMS network architecture.

2.2 Malformed Message Attacks in IMS

Protocols, among others, define specific rules and grammars for their messages. For the scope of this work any message violating the protocol's definitions is defined as 'malformed'. As already mentioned, IMS relies on SIP for session management. Consequently, malicious users may try to exploit SIP messages in order to launch a malformed message attack, similar to the conventional SIP-based services (Wieser and Laakso, 2003), (Dimitris Geneiatakis et al., 2007).

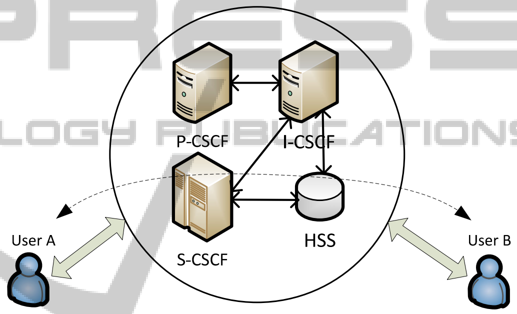

Figure 1: IMS core network architecture. Users contact P-CSCF in every request, which is responsible to contact I-CSCF to locate user's home network.

The freedom of SIP message structure (according to the SIP grammar) and its text format, offer to malicious users the chance to develop numerous non SIP conformed messages. For instance, a malicious user might not include values in the mandatory fields of a SIP message, or include inappropriate values, or even craft a message composed of lengthy optional information in order to cause buffer overflow.

In another example a malicious user may insert multiple or NULL headers, in order to introduce delays in routing decisions or other unexpected incidents affecting system's availability. Furthermore, the latter user may also craft such a message by inserting malformed UTF8 sequences in header fields or by overflowing the messages with special characters. Figure 2 depicts different examples of malformed messages. Note that the target of a malicious user can be any of the IMS components or even a traditional networking communication component that IMS interconnects with NGN.

INVITE nvrakas@ unipi.gr Via: SIP/2.0/UDP [1050::::0005::120c:354b] Max-Forwards: 70 From: <sip:nvra_private@unipi.gr>;tag=589f Call-ID: ak5fj49fhujDUuf0AjU9 Call-ID: ak5fj49fhujDUuf0AjU7 Call-ID: ak5fj49fhujDUuf0AjU8 From: <sip:dgen_private@unipi.gr>;tag=589f	INVITE tel: + �������□ □ □ □ Via: SIP/2.0/UDP [1050::::0005::120c:354b] Max-Forwards: 70 From: ���������������� ���� □ �□ ����□ □ □ �□ □� □ �□�□ □ □ ��□ □ □ ��□ □

Figure 2: Examples of SIP malformed messages. The first message contains multiple call-id, which is used to uniquely identify a call, while the second message includes inappropriate values.

3 OPEN IMS EVALUATION

To assess open IMS robustness against malformed message attacks we employ, in a local network, the architecture depicted in Figure 3. The open IMS platform was installed on an Intel core 2 at 2.4Ghz machine with 4 GB RAM, while the IMS legitimate users were installed on an Athlon 3 core at 2.4GHz with 2GB RAM, and the attacker on an Intel Pentium 4 at 2.8GHz with 2 GB RAM. All the systems were running Ubuntu O/S.

We employ two main categories of malformed message attacks based on the main targets of the attacker. In the first category the malicious user targets the registration procedure, while in the second one targets the main service, by creating different SIP malformed REGISTER and INVITE messages respectively.

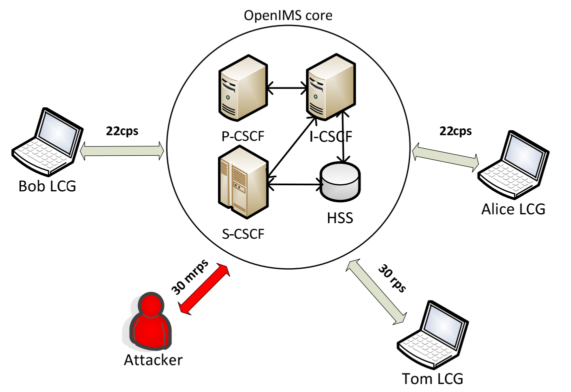

Figure 3: The open IMS test bed that has been employed for evaluating the robustness of the architecture.

Table 1 briefly describes the employed attack scenarios. In all of them there is some background traffic (*bgt*) of 22 new multimedia sessions per second between Bob and Alice, while the minimum duration per session is 5 seconds. Therefore, the concurrent background media sessions are approximately 110 (5*22 = 110). To compare the attack outcomes we employ one additional scenario for both targets (registration and main service), named *adlt-r* and *adlt-i* respectively, where user Tom generates 30 legitimate sessions (adlt) per second. We run all scenarios for a time period of one hour each.

At this point it is important to stress the differences between the two attack testing suites. In our testing suite we utilize messages with multiple header values while the PROTOS attack tool includes overflows of special and non-ascii characters, as well as ANSI escape and malformed utf-8 sequences.

We evaluate the open IMS robustness against malformed message attacks by measuring:

a) The introduced overhead legitimate users experience, and
b) the open IMS memory consumption.

In the following subsection we describe the results of the tests performed.

Table 1: Malformed message attack scenarios employed for Evaluating Open IMS robustness.

	Sc No.	Description
INVITE Malformed	S1	In this scenario we generate a traffic of 30 malformed SIP INVITE requests per second, using the PROTOS malformed message testing suite.
	S2	In this scenario we generate 30 malformed SIP INVITE requests per second, using our malformed message testing suite.
REGISTER Malformed	S3	In this scenario we generate a traffic of 30 malformed SIP REGISTER requests per second 30 using our malformed message testing suite

3.1 Server Side Memory Consumption

Figures 4 and 5 illustrate open IMS memory consumption for the case of malformed REGISTER and INVITE message attacks correspondingly.

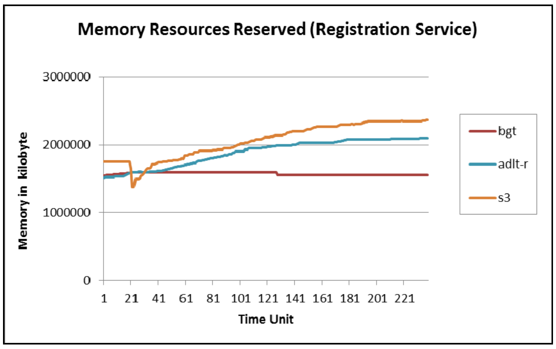

Figure 4: Memory consumption in registration service during attack scenarios. There is an increase of 9% compared to additional legitimate traffic scenario.

The PROTOS malformed message testing suite has not any impact on the open IMS memory resource consumption for both attack targets (registration and main service). Open IMS effectively discard such kind of messages reacting on PROTOS malformed

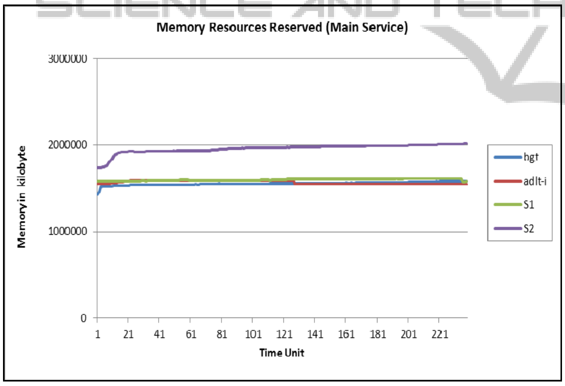

Figure 5: Memory consumption in main service during attack scenarios. There is an increase of 25% compared to additional legitimate traffic scenario.

messages similar to well-formed messages. This response was in a way expected as open IMS is built on SIP Express Router (SER) (www.iptel.org) in which various extensions have been introduced in order to enhance it against this type of malformed message attacks. However, in the case of our malformed message attacks testing suite there is an increase in memory consumption of 25% in the case of targeting the main service, while when the target is the registration service there is an increase of up to 9%, compared to the additional legitimate traffic (addl-r).

The results reveal that the host's system memory is barely affected by any kind of attacks to the S-CSCF. In fact the registration service should be reached even by an external attacker since everyone is considered external until its successful registration. Open IMS proved robust enough to evade such attacks with an acceptable overhead in memory consumption. Another point is that the S-CSCF discards the messages that do not include authentication header given that the NASS-IMS-Bundled Authentication (NIBA) (3GPP 2010) is disabled by default. During the execution of our attack scenarios it is worth stressing that open IMS has not crashed.

3.2 Client Side Effects

Similarly to the memory consumption results, the end-to-end delay experienced by the users in the case of attacks launched through the PROTOS test suite is negligible; approximately 0.5 %. On the other hand, when the IMS is under attack through our malformed message attack tool, the end-to-end delay is increased by 4000 %, in the case of INVITE malformed message attacks and by 300 % during REGISTER malformed message attacks.

Figures 6 and 7 depict the average response times. Considering Figure 8, we draw the conclusion that open IMS tends to be susceptible to our testing suite.

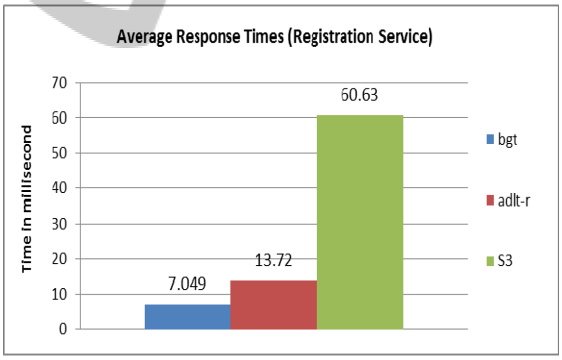

Figure 6: The end-to-end overhead imposed to user when the registration service is under attack. There is an increase up to 300%.

Virtually all (over 95 %) of the legitimate sessions became fragile due to the large amount of introduced delay. Constantly the majority of the sessions ware experiencing response time of over 100ms and with an average time of 413ms. It is straightforward that an internal attacker can decrease the QoS introducing such a considerable amount of delay to media sessions.

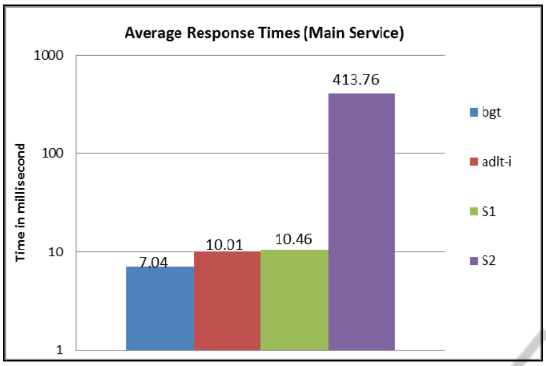

Figure 7: The end to end overhead imposed to user when the main service is under attack. There is an increase up to 4000%.

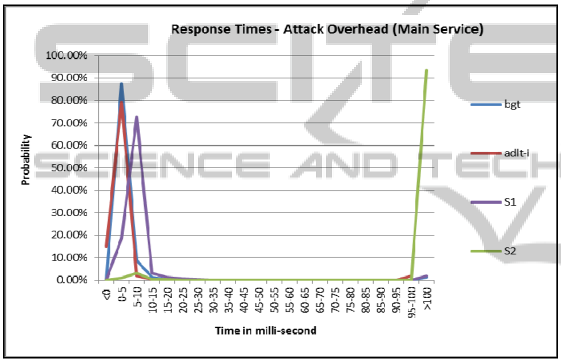

Figure 8: Probability density function for end to end delay in the case of IMS main service. During the attack scenarios almost all legitimates session impose a delay of more than 100 milliseconds.

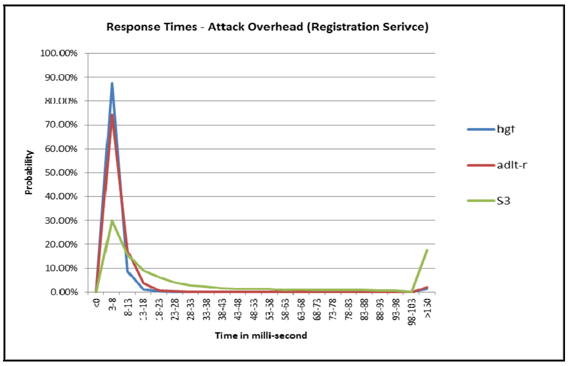

Figure 9: Probability density function for end to end delay in the case of IMS registration service. During the attack almost the 70% of registrations require more than 150 milliseconds.

Considering the probability density functions illustrated in Figure 9 we infer the erratic behavior of the open IMS core during scenario3. Specifically, our malformed requests confused the message parser and the latter became unable to keep a consistent serving pace: Only 30 % of the legitimate sessions were established with an acceptable delay time while the rest 70% of the sessions were established experiencing an excessive delay of more than 100ms. It is straightforward that the CSCF is able to deter PROTOS test cases that are mainly consisted of sequences of special and non-ascii characters. On the other hand the multiple headers of our suite introduces excessive delays to the media sessions. Therefore we can assume that the implementation of the parser is not versatile enough to face new types of malformed attacks but only the well-known ones.

4 CONCLUSIONS & FUTURE WORK

In this paper we evaluate open IMS robustness against malformed message attacks. Open IMS assessment results indicate that even though attacks based on well-known malformed messages have no impact on IMS performance, there are still malformed message attacks to which IMS proves to be vulnerable. From our perspective solutions such as those proposed in (Dimitris Geneiatakis et al., 2007) and (Niccolini et al., 2006) could be employed to eliminate malformed message consequences in sip based environments such as IMS. However, even these solutions are not able to detect new kind of malformed message attacks. For this reason, additional protection mechanisms are necessary for enhancing the existing IMS security level, against malformed message attacks, and minimize the chances for unauthorized access or even denial of service.

REFERENCES

3GPP, 2008. TS 23.228: IP Multimedia Subsystems (IMS), Third Generation Partnership Project, *Technical Specification Group Services and System Aspects*.

3GPP, 2010. TS 33.203: 3G security; Access security for IP-based services (Release 10): Third Generation Partnership Project, *Technical Specification Group Services and System Aspects*.

Geneiatakis, D. et al., 2006. Survey of security vulnerabilities in session initiation protocol. *Communications Surveys & Tutorials, IEEE*, 8(3), 68-81.

Geneiatakis, D. et al., 2007. A framework for protecting a SIP-based infrastructure against malformed message attacks. *Computer Networks*, 51(10), 2580-2593.

Keromytis, A. D., 2010. Voice-over-IP Security: Research and Practice. *IEEE Security and Privacy*, 8(2), 76-78.

Niccolini, S. et al., 2006. SIP intrusion detection and prevention: recommendations and prototype implementation. In *VoIP Management and Security, 2006. 1st IEEE Workshop on*. VoIP Management and Security, 2006. 1st IEEE Workshop on. pp. 47-52.

OSVBD, 2007. Asterisk SIP channel driver SIP malformed UDP packet DoS. Available at: http://osv db.org/show/osvdb/34482.

Rosenberg, J. et al., 2002. SIP: Session Initiation Protocol, RFC 3261.

Wieser, C. and Laakso, M., 2003. Security Testing of SIP Implementations, 1--2003