Securing IP Multimedia Subsystem with the appropriate Security Gateway and IPSec Tunneling

Dominik Slezak[1] and Yvette E. Gelogo[2]

Abstract

In this paper we presented the security vulnerabilities, threats, and possible attacks for IP Multimedia Subsystem and the appropriate Security Gateway and IPSec Tunneling. Multimedia Subsystemis an architectural framework for delivering Protocol services is in need of more secure connection between interconnected networks. IMS unifies applications that are based on SIP (Session Initiation Protocol), a next-generation packet-based signaling protocol that enables rich multimedia sessions (voice, images, and video).The proposed solution is based on the definition of a Security Gateway for the internetworking between IMS and the Internet. The main functions to be performed by the SEG are discussed, and then the security procedures are briefly presented.

Keywords : IP Multimedia Subsystem Session Initiation Protocol (SIP), Security Gateway (SEG), IPSec Tunneling

1. Introduction

IP Multimedia Subsystem is an architectural framework for delivering Protocol services. It was originally designed by the wireless standards body Generation Partnership Project as a part of the vision for evolving mobile networks beyond Its original formulation (3GPP R5) represented an approach to delivering "Internet services" overThis vision was later updated by 3GPP ,requiring support of networks other than GPRS, such asLAN ,and fixed line.

Third Generation (B3G) networks aim to merge two of the most successful paradigms in communications: cellular networks and the Internet. The IP Multimedia Subsystem (IMS) is the key element in the B3G architecture that makes it possible to provide ubiquitous cellular access to all the services that the Internet provides. The goal of IMS is to support all the services, current and future, that the Internet provides.

The IMS principles foresee a complete migration towards an all-IP architecture, in which both the user and the control plane are based on the IP protocol stack. In particular, the control plane and the call control

Received(April 25, 2011), Review request(April 26, 2011), Review Result(1st: May 19, 2011, 2nd: May 27, 2011)
Accepted(June 30, 2011)

[1]Chief scientist, Infobright Inc., Canada
email: slezak@infobright.com

[2](Corresponding Author) 306-791, Department of Multimedia Engineering, Hannam University
email: vette_mis@yahoo.com

functions will be supported by the Session Initiation Protocol (SIP).IMS unifies applications that are based on SIP (Session Initiation Protocol), a next-generation packet-based signaling protocol that enables rich multimedia sessions (voice, images, and video).

The NDS provides IP security between different domains and nodes within a domain. Integrity and possibly confidentiality of information exchanged between entities internal to a domain are protected by the IPSec protocol via the creation of specific Security Associations (SAs). Traffic entering and leaving a domain passes through a Security Gateway (SEG). A SEG is responsible of the application of the security policies on the traffic incoming to and outgoing from the SD; such policies may also include packet filtering and/or firewall functionality. Each SEG maintains IPSec SAs with other SEGs of other domains [5].

2. Background

IP Multimedia Subsystem (IMS) is an architectural framework for delivering internet protocol multimedia to mobile users. IMS defines a complete architecture and framework that enable convergence of voice, video, data and mobile network technologies over an IP-based infrastructure filling the gap between two successful communication paradigms, cellular and internet technology. The convergence of voice and data networks, fixed and mobile communication is a great achievement in the communication world with advantage to maintain single communication platform for all but the big challenge is to maintain an adequate security level in the heterogeneous network environment. However, the current solutions, like firewalls, anti spy ware and antivirus systems, failed to counter the emerging threats because they only target specific types of threats. The proposed security architecture to IMS counter both, known and unknown threats, but along with other deficiencies like creativeness with previous solution [3].

The current generation of mobile devices should perform well when using the media plane security architecture specified by 3GPP [4].

The IP Multimedia Subsystem (IMS) is an open IP based service infrastructure that enables an easy deployment of new rich multimedia services mixing voice and data. The IMS is an overlay network on top of IP that uses SIP as the primary signaling mechanism. As an emerging technology, the SIP standard will certainly be the target of Denial of Service (DoS) attacks and consequently IMS will also inherit this problem [3].

The IMS architecture presents significant security challenges that must be addressed by the carriers as IMS moves into widespread deployment. The generally open and distributed architecture creates the advantage of flexibility in implementation and deployment. It also creates a multitude of interface points that must be secured. Security around the IMS is a significant part of the 3GPP standards work. The 3GPP working group responsible for overall security analysis is TSG SA WG3. In particular, this group is charged with considering

new threats introduced by the IP based services and systems and setting the security requirements for the overall 3GPP system [7].

3. Security Risks

3.1 Risks to the Application Service Layer

Since applications are typically hosted on networked servers running conventional operating systems, they are vulnerable to the same type of threats as enterprise businesses experience. For example, a "Push-to-Talk"application running on a Linux-based server, or an Instant Messaging or VoIP Call Management application on a Windows-based server are all vulnerable to the same threats as their enterprise counterparts experience on a daily basis, such as a Denial of Service (DoS) intrusions, viruses, or worms proliferation that ultimately can impact uptime and cost carriers service revenue. An inability to effectively address specific security issues in the Application Layer limits a carrier's ability to provide enhanced services to customers.

3.2 Risks to the Control Layer

The SIP protocol is managed in the Control Layer where there are specific types of attacks that can be launched against SIP elements in the IMS network. Any device that uses IP to communicate with the IMS network can send traffic to this layer and launch an attack

3.3Risks to the Transport Layer

One of the most common risks to the Transport Layer is from a flood of data packets that consume a network's entire bandwidth and cause it to perform poorly. This type of flood can occur using any of the available network protocols such as a TCP Flood (also known as a SYN Flood) or a UDP Flood, among several others.

3.4 Risks to the Access Layer

Personal computers and new "Smartphone" mobile are key network entry points for security threats which, once connected, allow a hacker to propagate infection to other endpoints on the IMS network.

While the security risks to personal computers are well recognized the risk to wireless Smartphone is not well understood, these devices are now the targets of similar threats as their desktop or notebook counterparts. This includes threats such as viruses, worms, Trojan horses, Adware, Spyware and spam.

4. Classification of Attacks

4.1. Violation of confidentiality

a. Eavesdropping user traffic

This attack utilized by an intruder to intercept the information flows emitted by the two legitimate users involved in a SIP session. This effect is obtained by means of the generation of a re-INVITE SIP message in which the IP addresses and possibly the dialog parameters are modified with respect to those exchanged in the original SIP setup phase.

b. Compromise of location information.

This attack is based on the vulnerability of the 3xx response messages.

The intruder emits a 302 moved temporarily message assuming the identity of the destination contained in the INVITE previously emitted by the victim. By inserting his own IP address in the field "Contact"of the SIP header of the 302 response, the attacker re-directs towards himself the successive requests emitted.

c. Eavesdropping signaling

In this attack the intruder aims at impersonating a SIP Proxy Server. The reception of a 305 Use Proxy response indicates to an UAC that a specified resource has to be reached by means a Proxy specified in the field "Contact". When this event occurs, the UAC has to present a new request properly modified according to the indications contained in the 305 Use Proxy message.

4.2. Denial of service (DoS)

a. Tearing down a session

This kind of attack aims at tearing down a SIP session previously established between two victims. This attack needs a preliminary phase in which the intruder sniffs the dialog parameters (From, To, Call-ID). Once the values of these parameters are known, the intruder emits a BYE message towards both the legitimate users. The emission of these two messages will cause an unexpected tear down of the SIP session.

b. Modifying a session

This attack uses the re-INVITE message to modify the SIP session parameters (e.g. the audio/video codecs)

so as to inhibit the session parties to correctly receive the multimedia flows. Normally, the session parameter negotiation is performed by means of a three-way-handshake procedure taking place during the session setup. The session parameters are contained in the SDP body of the INVITE, 200 OK and ACK messages. In particular, the UAC insert in the INVITE message the list of supported media capabilities, whereas, the UAS responses with a 200 OK message containing those capabilities that are accepted for the session.

c. Cancelling a session

Aim of this type of attack is to make unattainable a UA by deleting the SIP request directed to it. The attacker emits a CANCEL message just before that the UAS emits the definitive response (200 OK messages) to an INVITE sent by a UAC. This a mandatory condition for the success of the attack, otherwise the reception of the CANCEL message will not have any effect on the UAS. The attacker sniffs the communication channel and, whenever an INVITE addressed towards a specified UAS is revealed, a CANCEL message carrying the same session parameter is emitted so as to make impossible the session setup.

d. SIP DoS attack and amplification

This attack aims at directing a huge amount of SIP signalling traffic towards a network element so as to make it unusable. In particular, this effect can be obtained by issuing a set of SIP requests, with a false source address, towards a set of destinations. Each message contains the address of the victim in the "Via"field. In this way, all the responses of the destination parties will be addressed towards the victim so as to cause the saturation of its processing capabilities.

4.3. Unauthorized access to service

a. Registration hijacking

Registration hijacking means that the attacker may do malicious registrations to the registrar. Attacker may for example register his own device as the contact address of the victim and deregister all old contacts. After that all requests to victim direct to the device of the attacker. In this case the victim is an IMS terminal currently located in Internet.

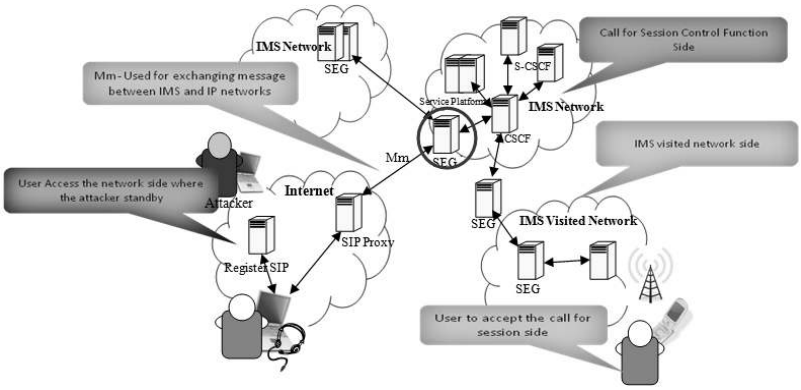
b. 3xx response code

By means of this attack an intruder aims at assuming the identity of the called user. The 3xx responses provide information of the current location of the victim, so an attacker can send the victim a 3xx response by assuming the identity of the original destination of the INVITE by indicating in the field "Contact" his own IP address.

5. Proposed Solution

This section deals with the description of a possible guideline for implementing efficient countermeasures to face with the security attack. With the proper Security Gateway positioning the possible threats and attack will be mitigated.

The proposed solution is based on the definition of a Security Gateway for the internetworking between IMS and the Internet. In the following the main functions to be performed by the SEG are firstly discussed, and then the security procedures are briefly presented.



[Fig. 1] Security Gateway (SEG)

5.1 Security Gateway (SEG)

The lack of any adequate system of security enforcement on the Mm reference point and on the signalling traffic passing through the Internet can be exploited by an attacker on the Internet to carry out attacks over the SIP signalling.

1. NA (P) T-PT

The Network Address (and Port) Translator-Protocol Translator (NA(P)T-PT) uses a pool of IPv4 addresses to be associated to IPv6 nodes when a session crossing the IPv4/IPv6 boundaries is set up. The IPv4 to IPv6 (and vice versa) binding allows a transparent routing between the two IP domains without the need to modify any of the end-points of the communication.

2. IPv4/IPv6 internetworking

Since IMS requires the use of IPv6 protocol, while IPv4 is still widely used in the Internet, IP level and application level internetworking is an aspect that has to be solved at Mm interface. The IP level internet working could be solved by a Network Address (and Port) Translation (NA (P) T). As for application level address translation, an Application Level Gateway (ALG) should be used.

3. Protection SEG

It is the SEG component specialized in the resolution of the previously listed attacks and security issues. It can be integrated in the IMS ALG, since it works at application level.

4. Signaling adaptation between 3GPP profile of SIP/SDP and non-3GPP SIP/SDP standard.

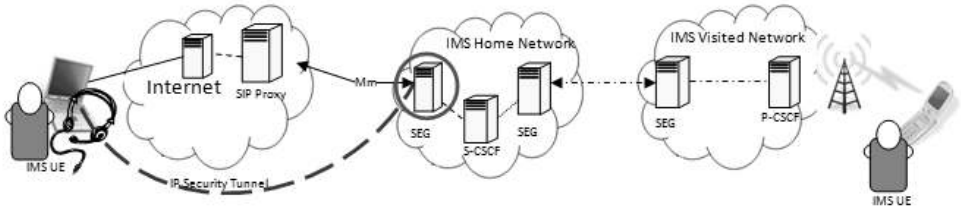
The 3GPP introduced a few header extensions into the SIP protocol to allow its usage within the IMS procedures. To grant a correct inter working with non-IMS SIP terminals, the signaling extension headers should be properly treated, since a standard SIP User Agent would not understand the 3GPP extensions.

5.2 SEG Inter working

In this section the security aspects of IMS inter working with the Internet are examined. All the mechanisms for signalling and addressing were analyzed. Further, we assume that the security mechanisms used in the IMS core network assure a good level of security, while no security procedure is deployed in the Internet. Before going out to the network itself, it must be secure, there should have a direct and secured tunnel.

The red dotted line indicates the new proposed IP Security Tunneling.

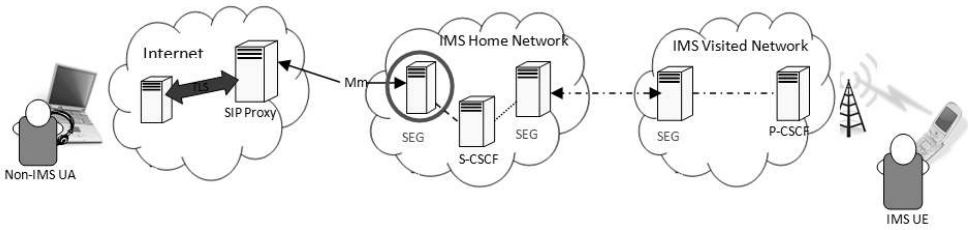
1. IMS UE in the Internet



[Fig. 2] IMS-UE in the Internet

To guarantee an adequate level of protection to the signalling going across the Internet, the IMS UE in the Internet should register to its home network via an IPSec tunnel established with the SEG.

2. SIP UA call towards an IMS UE over IMS network

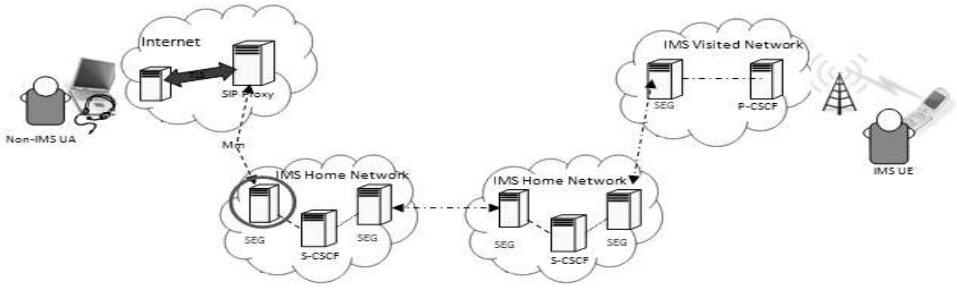


[Fig. 3] IMS-UA in the Internet

SEG should not accept non-IMS UA session without using any security mechanism. It should be rejected by SEG and send an error message requiring a security or there should have an authentication that the incoming session is allowed. Then the UA should retry the session setup using TLS. The SEG must check whether TLS has been used over all the hops between the terminal and the SEG itself. This check is executed by assuring that the entire sip URIs listed in the via header field are sips.

3. IMS UE over IMS network initiating a call towards a SIP UA in the Internet

TLS in the hops from the I-CSCF to the non-IMS UA is requested by the 3GPP standards is in used. If one of the proxies in the Internet cannot offer TLS, it must answer with an error message telling that the non-IMS UA has failed to offer TLS. The SIP standard recommends the UAs to support TLS, but this is not a mandatory requirement; anyway, the last hop preceding the UA, receiving a sips URI in the request URI, must relay the message in any secure mechanism to the UA or answer with an error message. sips URI allows resources to specify that they should be reached securely.



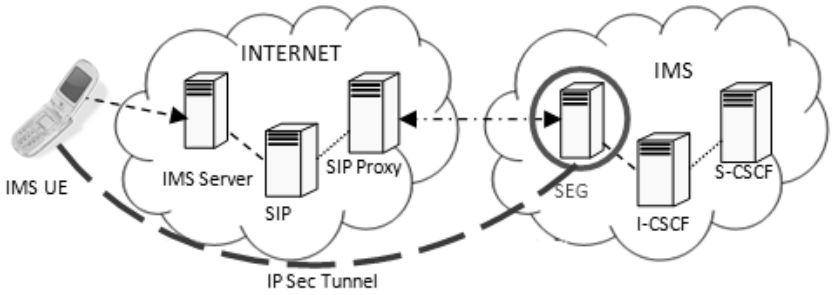
[Fig. 4] Call initiated by a SIP UA in the internet

5.3.IMS UE security procedures

The security aspect in SIP toward non-IMS terminal connections in the internet is vulnerable to threats in this case, there is a need to examine the IMS terminals trying to access to its home network via Internet

First Solution:

Access granted by a SIP network in the Internet to locate the correct SEG to reach the IMS home network. Since any IMS UE is SIP compliant, it can use the SIP proxies in the Internet to locate, hop by hop, the SEG – which is itself a SIP proxy – via NAPTR/SRV DNS procedures.



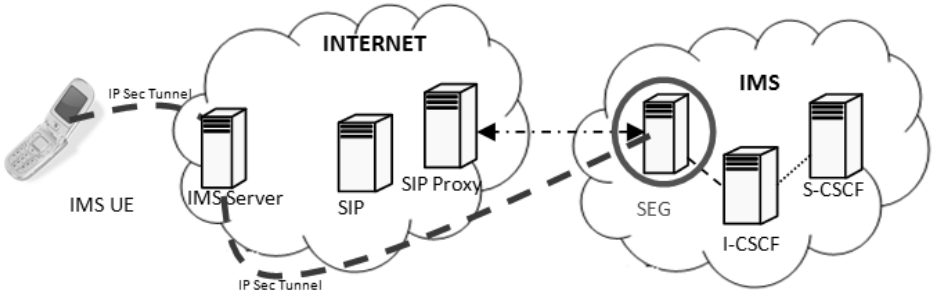
[Fig. 5] IPSec tunnel between SEG and IMS UE

Second Solution:

The second solution is based on the assumption that the internet SIP provider has an agreement with the IMS provider and implements an IMS server offering the SEG location function for all the IMS core networks having subscribed an agreement.

Third Solution:

The IMS server in the Internet has a permanent static IPSec tunnel towards each SEG.



[Fig. 6] Permanent static IPSec tunnel towards each SEG

6. Conclusion

In this paper we presented the security risk, threats and vulnerabilities over the IMS network. The possible attacks were classified. Security aspects arising from a scenario in which IMS network inter operate with an open IP network like Internet have been examined. In particular, possible security threats related to SIP protocol have been classified and described. Some possible solutions were presented in order to mitigate the vulnerabilities, threats and attacks of the network. Finally, more secure connection by additional and proper security gateway tunnelling was conceptualized.

References

[1] 3GPP TSG SA WG3 Security — S3#37 S3-050035, February 21 - 25, 2005, Sophia Antipolis, France

[2] Exploring IMS Network Security for Next Generation Network (NGN) Carriers, A Fortinet White Paper

[3] Kalyani Chalamalsetty, "Architecture for IMS Security to Mobile: Focusing on Artificial Immune System and Mobile Agents Integration", Master Thesis Computer Science Thesis no: MCS-2009:24 May 22nd 2009.

[4] PrajwolKumar Nakarmi, "Evaluation of VoIP Security for Mobile Devices in the context of IMS", seNordSecMob–Master's Programmein Security and Mobile Computing

[5] M. Mogno, I. Petrilli, M. Listanti, "Vulnerability in IMS-Internet interworking: analysis and relevant solutions"

[6] 3GPP. Access security for IP-based services (release 7). Technical Report TS 33.203 V7.6.0, June 2007.

[7] 3GPP. Security architecture. Technical Report TS 33.102 V7.1.0, December 2006.

[8] S. Knuutinen: "Session Initiation Protocol security considerations". Seminar on Internetworking, Helsinky, Spring 2003. Available in http://www.tml.hut.fi/Studies/T-110.551/2003/papers.

[9] O. Rantapuska: "SIP call security in an open IP network". Seminar on Internetworking, Helsinky, Spring 2003. Available in http://www.tml.hut.fi/Studies/T-110.551/2003/papers.

[10] A. Steffen, D. Kauffman, A. Striker: "SIP security". Lecture notes in Informatics P-55, Bonner Kollen Verlag 2004, pp.397-410.

[11] 3GPP Technical Specification TS 33.203: "3G security. Access securityfor IP-based services". Available in: http://www.3gpp.org/specs/specs.htm.

Author

Dominik Slezak

He received his PhD in Computer Science in 2002 from Warsaw University, Poland. In an instructional capacity he has supervised more than 15 graduate students in Canada, Poland, and the United Kingdom. He has pursued academic collaborations with Warsaw University, University of Regina, and the Polish-Japanese Institute of Information Technology.

Yvette Gelogo

2006~2010 Bachelor of Science in Information Technology, Western Visayas College of Science and Technology.

Currently, Masters for Multimedia Engineering, Hannam University.

Research Interests: Ubiquitous Healthcare System Development, Mobile System Development and Design, Information Security, SCADA Security, Ubiquitous Learning, Biometric Authentication