International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Securing the IP Multimedia Subsystem with IPsec and HTTP Digest

Mohammed Ibrahim Omar*[a], Dr. Cheruiyot W. Kipruto[b], Dr. Michael W. Kimwele[c]

[a,b,c]*Computing and Information Technology (SCIT), Jomo Kenyatta University Of Agriculture And Technology, Kenya*

[a]*Email: eng.ibrahim2004@gmail.com*

[b]*Email: wilchery68@gmail.com*

[c]*Email: mkimwele@jkuat.ac.ke*

Abstract

Modern Telecommunication networks were combined from two communications: cellular networks and the Internet. The Internet Protocol Multimedia Subsystem (IMS) is the key element in the Modern Telecommunication networks architecture that makes it possible to provide wide range cellular access to all the services that the Internet provides. So, IMS 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 this different network environment. IMS is based principally on IP protocol. Therefore, it inherits the security issues of IP networks. The IMS architecture is open, distributed and it has the advantage of being flexible in its implementation and deployment. This generates a variety of communication interfaces, which can make the system very vulnerable to attack. Add to that, the services offered on the IMS network must be provided by ensuring confidentiality and respect the privacy of users. Therefore, it is necessary to secure the IMS network at every level of its architecture including the final customer or subscriber device. Solutions like firewalls, anti-spy ware and antivirus systems failed to counter the emerging threats because they only target specific types of threats. In this study we are proposing security approach which is a Combination model composed of two protocols IPsec and HTTP digest.

Keywords: Internet Protocol Multimedia Subsystem (IMS); Internet Protocol Security (IPsec); HTTP.

---

* Corresponding author.

1. Introduction

There are many different viewpoints and definitions for the IP Multimedia Subsystem (IMS). While many are promoting the IMS as a simple call control architecture easily implemented at the edge of the network, the 3rd Generation Partnership Project (3GPP) has defined a much more robust approach. There are many who believe the IMS is all about services. Yet others believe it is all about control. In reality, it is a little bit about both, but the primary purpose of the IMS infrastructure is to provide session control at the core of the network while enabling other support needed to provide those services, regardless of media type [1]. Third Generation (3G) networks aim to merge two of the most successful paradigms in communications: cellular networks and the Internet. The IP (Internet Protocol) Multimedia Subsystem (IMS) is the key element in the 3G architecture that makes it possible to provide ubiquitous cellular access to all the services that the Internet provides. Picture yourself accessing your favorite web pages, reading your email, watching a movie, or taking part in a videoconference wherever you are by simply pulling a 3G hand-held device out of your pocket. This is the IMS vision [5].

2. Architecture of IP Multimedia Subsystem

The IMS permit the convergence and the integration of data and multimedia services like voice over IP (VoIP), video, presence, instant messaging and so on. Multiple protocols are used with IMS but the main one is SIP protocol (Session Initiation Protocol). It provides method for configuring and controlling multimedia applications in IP network. The IMS architecture include four layers (Fig 1), which work together to provide reliable service [7].

Figure 1: IMS layered architecture.

According to the traditional definition, network security comprises integrity, confidentiality, and availability. Message integrity ensures that if an unauthorized party modifies a message between the sender and the receiver, the receiver is able to detect this modification. In addition to message integrity, integrity mechanisms always provide some type of proof of data origin. Knowing that a message has not been modified without knowing who

initially created the message would be useless.

Confidentiality mechanisms keep unauthorized parties from getting access to the contents of a message. Confidentiality is typically achieved through encryption. Denial of Service (DoS) attacks compromise the system's availability by keeping authorized users from accessing a particular service. The most common DoS attack consists of keeping the servers busy performing an operation or sending the servers more traffic than they can handle [5]. 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].

3. Security Threats in an IMS networks

Security issues in the IMS network is an important challenge as it includes a wide variety of services, protocols and components. This complexity enhances the number of vulnerabilities and risk for the IMS users and the ISP. Some of these vulnerabilities are inherent on one hand to protocols and services used and others are induced by the context of the IMS like users mobility. On the other hand, Quality of Service (QoS) is also big challenge in any IMS network as this network is designed to offer time sensitive application like video, videoconferencing and so on. The main idea in this paper is to secure IMS in the access layer [2]. IMS is based principally on IP protocol. Therefore, it inherits the security issues of IP networks. The IMS architecture is open, distributed and it has the advantage of being flexible in its implementation and deployment. This generates a variety of communication interfaces, which can make the system very vulnerable to attack. Add to that, the services offered on the IMS network must be provided by ensuring confidentiality and respect the privacy of users. Therefore, it is necessary to secure the IMS network at every level of its architecture including the final customer or subscriber device [4]. There are a number of security threats already established for IP networks (and well exploited).These attacks can be prevented through the practices discussed in this chapter and do not necessarily require huge investments to prevent. The main threats today are [1].

- Eavesdropping
- Registration hijacking
- Server impersonation
- Message body tampering
- Session tear-down
- Denial-of-service
- Amplification

3.1 Eavesdropping

Eavesdropping lets hackers intercept SIP messages without detection. This method is used by hackers to obtain sensitive information such as routing and private user identities. The information is then used to create new messages that will pass authentication unless there are other forms of authentication and security (as we will continue to discuss). The eavesdropping is prevented through encryption, both within the secure home domain as well as across transited networks. Encryption is the best means to prevent eavesdropping from occurring and is one of the reasons that IPv6 with IPsec has been defined for use within the IMS [1].

3.2 Registration Hijacking

Registration hijacking occurs when a *REGISTER* message is sent by a hacker with a subscriber's stolen identity. The identities are learned through eavesdropping and serve to move a current registration to another location or establish an entirely new registration if the legitimate subscriber is not connected and registered. Once registered, the attacker has full access to the same services as the legitimate subscriber [1].

3.3 Server Impersonation

Server impersonation allows a proxy server in another network to ―pose‖ or masquerade as another legitimate proxy redirecting all traffic to itself and away from the legitimate proxy. In the IMS domain, this would mean compromising the CSCF function and redirecting requests and responses to the rogue CSCF. We see this form of attack in the Internet domain already. Web sites that are masquerading as legitimate Web sites are used to coax sensitive information from unsuspecting consumers. This could become a major problem within the IMS if there is no means to verify the network. Procedures are defined for IMS that allow the user device to authenticate the IMS network to ensure it is communicating with the trusted domain of the service provider (or authorized partner). There are other measures we will talk about later that help prevent this as well [1].

3.4 Message Body Tampering

Tampering with the message body requires access to the message body, which without encryption is very easy. Since SIP is sent in plain text (rather than binary coded), it is very easy to eavesdrop on a SIP network and read the contents of the messages. Depending on the type of SIP message, this has varying consequences. If the message body contains a text message containing the message ―call me‖ and provides a telephone number, the text message could be modified and delivered to the destination with a different number. The receiver would then respond back to the rogue subscriber rather than the legitimate sender of the message. There are many other examples of how this method could be used to steal identities and obtain personal information from unsuspecting subscribers. [1]

3.5 Session Teardown

Tearing down sessions is a disruptive attack that if launched to a wide range of subscribers could have serious implications. For example, if this were carried out in concert with a major catastrophic event, communications

for thousands of people would suddenly be compromised, as they would have been "cut off" and attempting to reconnect would congest the network [1].

3.6 Denial-of-Service Attacks

Denial-of-service attacks take many forms and of course can also be very damaging. These types of attacks flood the network to the point where legitimate subscribers can no longer gain access to the communications services they need, eventually leading to the shutdown of many systems when they reach their capacity for traffic. One way of accomplishing this today is to send a request with a false or spoofed IP address and corresponding *VIA* header making it look like it came from a legitimate subscription. Sending the request to many different entities within the network would result in a flood of responses network-wide [1].

3.7 Amplification

Amplification is similar to denial of service with much broader coverage. The same request is sent to a redirect proxy, which then "splits" the request to many different directions, "amplifying" the number of responses in the network. Instead of having a response coming from one CSCF, the message is split and sent to many CSCFs. All of these security threats can be addressed through IMS and should be taken seriously by any IP-based service provider. It should be noted here that these attacks are not unique to IP-based services, though. We see many similar forms of attacks and security threats in the legacy telephone networks around the world today [1].

4. Problem Statement

Current telecommunication Companies use IP based systems which is a combination of two successful communication networks: Mobile networks and the Internet. The IP Multimedia Subsystem (IMS) is the key element in this architecture that makes it possible to provide ubiquitous cellular access to all the services that the Internet provides. So, IMS 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 this heterogeneous network environment. These telecommunication companies are suffering from hacking and breaching into their system by fake service providers. These fake service providers give the people free internet, free calls and sometimes very cheap international calls using internet.

5. Related works

To approach this problem, which is likely very complicated and varied proposed to model the network architecture of IMS as illustrated in Fig 1.

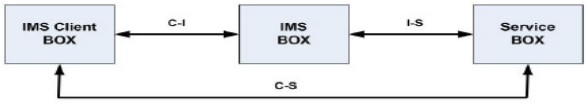

Figure 2: The Proposed model for IMS security architecture

This model includes the following components:

A) IMS client: it represents any user who connects to the IMS network in order to access a particular service offered by the network. A client accesses the IMS network via an access network which may be a telecommunication network or an IP network. In the case of the telecommunication network, the user has a SIM card that includes information used for authentication. In the case of IP network, wired or wireless, the user does not have a SIM card.

B) IMS-BOX is the core of the IMS network with its various internal components. We ignore the details of the communications and the various operations taking place in the core of the IMS network.

C) Service-BOX: represents the services in the IMS network for end customers. Basically, one IMS user connects in order to use service offered by Service-BOX [4].

These components communicate with each other via three interfaces:

***A) C-I Interface*:** between the IMS client and the IMS-BOX. It carries all the signaling and control traffic associated with client access to the IMS network. It is basically based on the SIP protocol.

***B) I-S interface*:** used between service platforms represented in the diagram by "Service-BOX" and the IMS core represented as "IMS-BOX". The traffic exchanged in this interface concern the verification of authenticity of the service platform. It also includes the authorization to offer service on IMS network. It is also based on SIP protocol.

***C) C-S interface*:** the interface is used to exchange media content between the client and the service platforms. This traffic can be a VoIP, video conferencing, video streaming or other. Protocols used on this interface depend on the service; it can be a HTTP, RTP and other [4].

5.1 Security Gateway

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 [6].

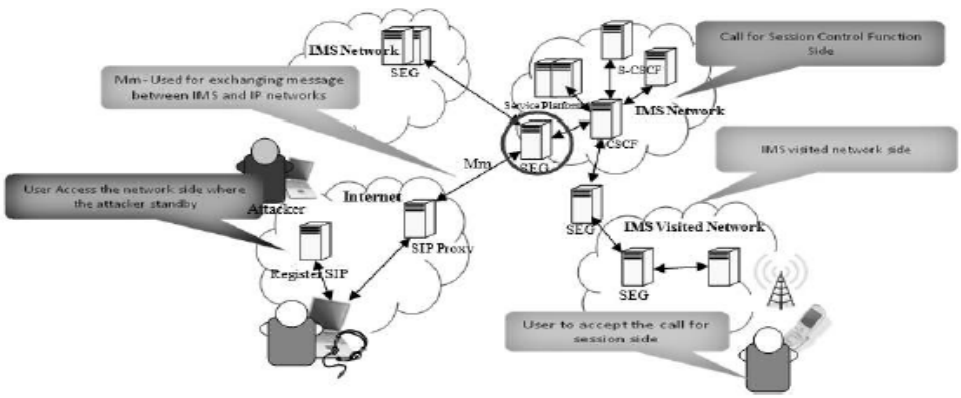

Figure 3: Security Gateway (SEG)

5.2 Security Gateway (SEG)

The lack of any adequate system of security enforcement on the Mm reference point and on the signaling traffic passing through the Internet can be exploited by an attacker on the Internet to carry out attacks over the SIP signaling [6].

5.3 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 [6].

5.4 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 internetworking 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 [6].

5.5 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 [6].

5.6 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 [6].

6. Security mechanisms

Currently, IMS security mechanisms use TLS7 or IPsec8 to provide authentication, integrity and confidentiality by securing SIP messages. These solutions can be used to secure the IMS Service delivery i.e. Trans - port Layer Security (TLS) for secure link between user and application server, Generic Bootstrapping Architecture (GBA)9 and Generic Authentication Architecture (GAA) to authenticate users before accessing services [9]. The TLS provides communications privacy over IP network and allows client/server applications to communicate securely against eavesdropping, tampering, or message forgery attacks. For IMS SDP, TLS could provide SIP message confidentiality and integrity protection against man in the middle and eavesdropping attacks. The 3GPP has recommended the use of GBA and GAA to authenticate users before accessing IMS services. By implementing this frame work the services can be protected against misuses [9].

The existing solutions have importance in their specific domains and protection against lower layers attacks. They did not provide security against higher layer attacks (i.e. session and application layer). A feasible solution that can degrade the efficiency of previously described attacks is the deployment of Intrusion Detection System (IDS) to enhance the existing security with protection against unauthorized access or misuse of IMS services. Since existing security mechanisms could not mitigate these attacks, an extended mechanism should be set out to enhance the security layer. To protect IMS system from attacks mentioned above, all incoming and out - going SIP messages must be processed by the IDS. If any message matches with the defined attacks rules, the message is blocked. In addition, the IDS will not allow further communication with illegitimate partner for a defined time. All the incoming SIP messages either from SIP stack or from SIP server are passed through the IDS entity that maintains database of active legitimate connections. This database is updated whenever a new user is attached to the IMS or is disconnected. Each SIP message is passed through an inspection filter which checks the pre - defined security rules for attack detection [9].

6.1 Proposed solutions

The proposed solution is composed of two protocols IPsec and HTTP digest,

6.2 HTTP Digest

When using digest access authentication the client and the server have a shared secret (e.g., a password), which is exchanged using an out-of-band mechanism. When a server at a given domain receives a request from a client the server challenges the client to provide valid credentials for that domain. At that point the client provides the server with a username and proves that the client knows the shared secret [5]. Clients using digest can prove that they know the shared secret without sending it over the network. Digest uses hashes and nonces for this purpose. A hash algorithm is a one-way function that takes an argument of an arbitrary length and produces a fixed length result, as shown in the following figure. The fact that hash algorithms are one-way functions means that it is computationally infeasible to obtain the original argument from the result. Two popular hash algorithms are MD5 and SHA1. A nonce is a random value that is used only once [5].

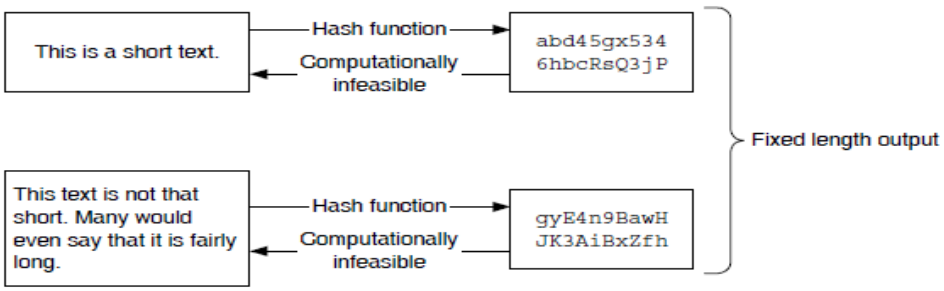

Figure 4: Hash function

Figure 3 shows how digest uses hashes and nonces. Alice sends an INVITE (1) request addressed to Bob

through her outbound proxy (at domain.com). The proxy challenges the INVITE with a 407 (Proxy Authentication Required) response (2). The proxy includes a Proxy-Authenticate header field with a set of parameters. The realm parameter indicates the domain of the proxy server, so that the client knows which password to use. The qop (quality of protection) parameter indicates that the server supports integrity protection for either the request line alone (auth) or for both the request line and the message body (auth-int). The server provides the client with a random nonce in the nonce parameter [5].

7. MD5 and hash

The algorithm parameter identifies the hash function (MD5, in this example). When the client gets the response it issues a new INVITE (3) with a Proxy-Authorization header field. The Proxy-Authorization header field contains a set of parameters. The response parameter is especially interesting. It contains a hash comprising, among other things, the username, the password, the server's nonce, the client's nonce (cnonce parameter), and the request line. When the auth-int qop is chosen the message body is also fed into the hash algorithm to generate the response parameter. When the server receives this Authorization header field it calculates another hash value using the same input as the client, but using the shared secret the server has. If the result matches the value in the response parameter of the INVITE request the server considers the authentication successful and keeps on processing the INVITE. Otherwise, the server will challenge this INVITE again. [5] The inclusion of random nonces chosen by the server in the hash prevents replay attacks. Even if an eavesdropper manages to obtain the correct hash value for a particular nonce it will not be able to access the server, since the server will challenge it with a different random nonce.

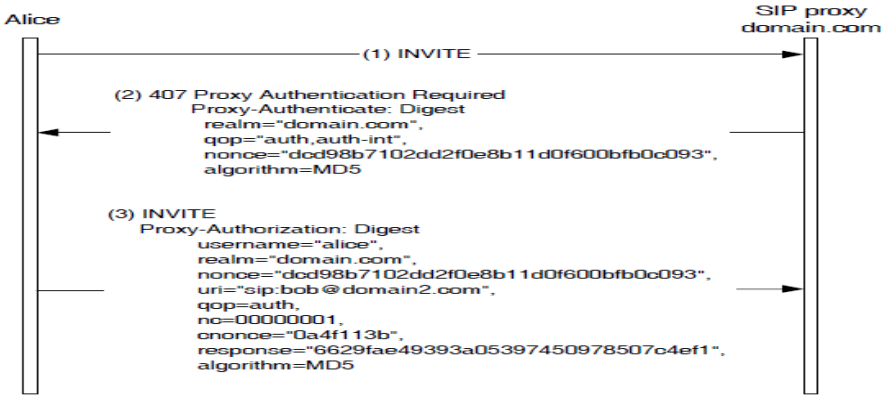

Figure 5: Digest operation

8. IPsec

IPsec provides confidentiality and integrity protection at the network layer. Nodes that want to exchange secure IPsec-protected traffic between them set up a so-called *security association*. A security association is identified by the addresses of the nodes and by its SPI (Security Parameter Index), and it contains the security parameters (e.g., keys and algorithms) that the nodes use to protect their traffic. IKE (Internet Key Exchange] is the key management protocol that is typically used to set up security associations [5].

8.1 ESP and AH

IPsec provides two protocols to protect data, namely ESP (Encapsulating Security Payload) and AH (Authentication Header). ESP provides integrity and (optionally) confidentiality while AH provides integrity only. The difference between the integrity provided by ESP and AH is that ESP only protects the contents of the IP packet (excluding the IP header) while AH protects the IP header as well. ESP adds to each IP packet a header and a trailer. The ESP header contains the SPI, the sequence number of the packet, and the initialization vector for the encryption algorithm. The ESP trailer contains optional padding in case it is required by the encryption algorithm and data related to authentication (i.e., integrity protection) of the data. [5]

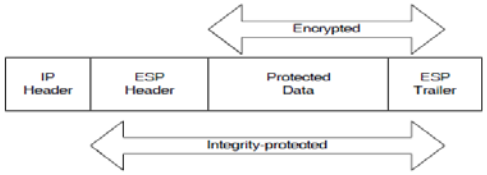

Figure 6: IP packet protected by ESP

8.2 Internet Key Exchange

Internet Key Exchange (IKE) is the key management protocol that is typically used to set up IPsec security associations. It is based on the ISAKMP (Internet Association and Key Management Protocol) framework, which defines how to exchange information with a peer in a secure way to perform key exchanges. IKE defines several such key exchanges, and the IPsec DOI (Domain of Interpretation) document defines which attributes need to be negotiated in an IPsec security association [5]. The establishment of an IPsec security association consists of two steps. In the first step, peers establish a security association to run IKE on it. In the second step, peers use this security association to securely agree on the parameters of the IPsec security association that will carry the actual data traffic [5].

9. Proposed protocols and models

The proposed protocols and algorithms will be used for each gateway routers of the three networks, IMS home network, IMS visited network and the internet.

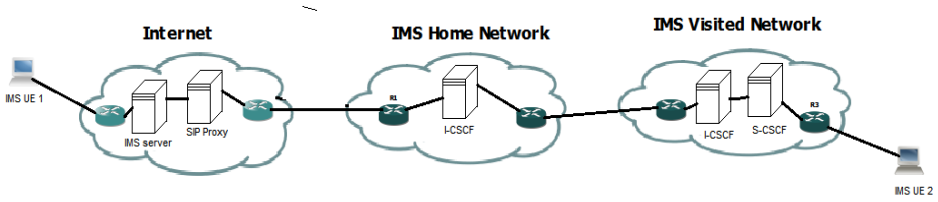

Figure 7: proposed solution (gateway router for each network)

To mitigate security threats in internet, whenever IMS UE1 wants to communicate with IMS UE2, IMS UE1

should first register to home network through IPsec tunnel with HTTP digest from the gateway routers

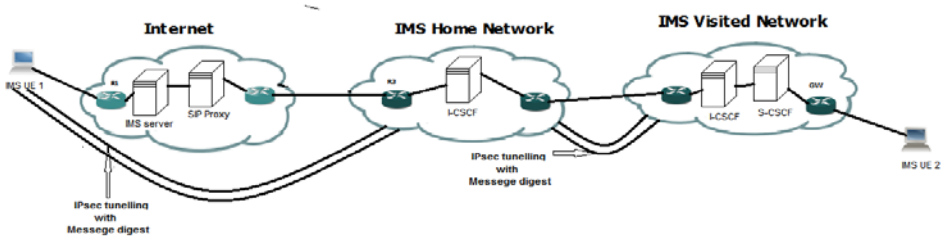

Figure 8: IMS UE1 communicating with IMS UE2 (Proposed solution)

10. Result

When we configured a gateway router for each of network using gns3 we get this result

R1

```
  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.0.1/255.255
.255.255/0/0)
  remote ident (addr/mask/prot/port): (192.168.1.1/255.255
.255.255/0/0)
  current_peer 23.0.0.3 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 13
   #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 12.0.0.1, remote crypto endpt.: 2
3.0.0.3
    path mtu 1500, ip mtu 1500
    current outbound spi: 0xD9E20149(3655467337)

    inbound esp sas:
     spi: 0x1C07125C(470225500)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: SW:1, crypto map: cmap
       sa timing: remaining key lifetime (k/sec): (4447711
```

R1

```
!
!
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 23.0.0.3
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 12.0.0.1 255.0.0.0
 ip ospf 1 area 0
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
```

Figure 9: Configured gateway router using MD5 ISAKMP KEY

5. Conclusion

In this study we presented security threats and attacks in an IMS networks and we a framework model for authenticating and encrypting the messages between two users using HTTP digest and IPsec protocols at each gateway routers. HTTP Digest provides authentication of users and a limited degree of integrity protection (no confidentiality). Digest integrity protects the request line and, potentially, the message body. Regarding availability, digest offers good DoS protection. Servers issuing challenges using digest can remain stateless until the new request arrives. IPsec provides confidentiality and integrity protection at the network layer. Nodes that want to exchange secure IPsec-protected traffic between them set up a so-called security association. In this paper we presented IPsec and HTTP digest to get Confidentiality, Integrity and availability (CIA) for gateway

routers at each network.

6. Recommendation

Our study focuses on accomplishing adequate security level and protecting the IMS networks from external world, but not focused internally. So we recommend further research on maintaining the security levels for IMS internally and externally to get robust security.

References

[1] Travis Russell. The IP Multimedia Subsystem (Session Control & Other Network Operations). New York Chicago San Francisco: McGraw-Hill Companies, 2008, PP 19-178.

[2] Chi-Yuan Chen, Tin-Yu Wu."An efficient end-to-end security mechanism for IP", Computer Communication,vol 3,pp 4259–4268, 2008.

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

[4] E.Belmekkia, B.Raouyane. "Towards a New Approach for Securing IMS Networks", Networks Labotatory, Institut nationale de Poste et Telecommunication, vol 4, pp 138 – 146, 2013

[5] Gonzalo Camarillo and Miguel A. Garcia-Martin. The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the cellular worlds. Chichester, England: John Wiley & Sons, 2006, pp 213-229.

[6] Gelogo, D. S." Securing IP Multimedia Subsystem with the appropriate Security Gateway and IPSec Tunneling". Journal of Security Engineering, vol 8, 2011, pp 306-791.

[7] Kai Shuang, Siyuan Wang." IMS Security Analysis using Multi-attribute Model". JOURNAL OF NETWORKS, VOL. 6 NO. 2, 2011

[8] Dong Wang and Chen Liu, "Model-based Vulnerability Analysis of IMS Network", Journal of Networks, vol. 4, no.4, June 2009.ETSI TS 102 165-1 V4.2.3, 2011-03

[9] Michail Tsag karo, T. D. "Securing IP multimedia subsystem: (IMS) infrastructures: protection against attacks". FITCE Congress., Session 07, Paper 05, 2008.