An approach to enhance security in the access layer of the IMS networks

E.BELMEKKI, M.BELLAFKIH, A.BELMEKKI

Abstract—Migration to next generation networks (NGN) is becoming more of a necessity for operators to follow the telecommunications industry evolution. However, NGN as it is proposed by the 3GPP pose significant challenges for the deployment. Indeed IMS architecture, that includes the core NGN, includes significant gaps in terms of security of users and services. For this purpose a complete security of different interfaces is a need to solve various problems in this field. In this context we propose in this work to highlight the vulnerability of IMS access layer, with an emphasis on possible attacks, before proposing a comparative study of existing security solutions. This work will provide a meaningful improvement of existing solutions to complete the process of securing user access.

Keywords— IP Multimedia System (IMS); IPSec, HTTPDigest, TLS, S/MIME, Session Initiation Protocol (SIP).

I. INTRODUCTION

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, 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 [1].

In this work we will first present the IMS network architecture and we propose a state of the art of the IMS network and SIP protocol. We will summarize the most critical attacks in the C-I interface in the access network level. We will focus on the analysis of the different solution to securing the SIP protocol [2]. Second, we will analyze experimentally the vulnerability in the C-I interface the experience is limited in the procedure for registration of a customer. Third, we propose in this paper a new approach to enhancing security in the access layer in IMS networks.

The paper is organized as following, Section 2, present architecture of the IMS network. Then, the Sections 3 present SIP protocol and his components. Section 4 and 5 describes the vulnerability and security in SIP with explications of each one. Section 6, Analysis and discussion about current security mechanism. Section 7, the security of the register method in the SIP protocol. Finally, future steps are discussed in conclusions.

II. ARCHITECTURE DE IMS

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 [3], which work together to provide reliable service.

• The access layer: The IMS user can access to IMS services through different access network like mobile network, wireless network, DSL line, enterprise network, etc. User can use basically different end IP based terminal to have access to IMS network, but can also use no IP based device.

• The transport layer: This layer offer an abstraction of different access network used which can be vendor technology dependent. It provides a unified network operation based on IP, unlike access network that can connect a no IP network users. It’s responsible for assigning IP address and registration for users. The upper layers in the IMS architecture use transport layer transparently without thinking to detail behind network access.

• The control layer: It is responsible for authentication, accounting and billing, routing SIP messages to the appropriate services and forwarding traffic (mainly associated with SIP) between transport and service layers and other IMS providers. The main components in this layer are: The CSCF (Call/Session Control Function), responsible for SIP interaction Home Subscriber Service (HSS), application servers and media servers. The CSCF is itself composed by tree components, each one assume different operation: P-CSCF (Proxy CSCF), I-CSCF (Interrogation CSCF) and S-CSCF (Serving CSCF). This layer includes also HSS which content subscriber data required for handling SIP session. The other component in this
layer is PCRF (Policy Control and Charging Rules Function) responsible for charging and control [4].

- The service layer: These layers provide multimedia service over IMS network. In the 3GPP specifications, the components of this layer are referred as service platforms. The communication between SCSCF and the service layer component are based on SIP.

In the article [5] we proposed a simplified Schematic Fig 1 IMS. In this scheme we present the most vulnerable interfaces in IMS like interface C-I, S-I and C-S. In this paper we propose an approach to securing the C-I interface to ensure confidentiality, the integrity and authentication. The protocols that circulated in this interface are DNS, DHCP and SIP. In the remainder of this work we concentrate in analysis of SIP protocol and we develop the different attacks related to this protocol in the context of IMS networks.

Fig. 1. Architecture of IMS simplified

III. THE PROTOCOL SIP

SIP is derived from the IETF through an RFC. It is used to initiate, modify and terminate the voice and multimedia sessions. SIP is located at the application level. To function, SIP requires additional standards and protocols. SIP is often described as a hat protocol since it is based on other protocol such as UDP [6] or TCP [7] in the transport layer. Figure 2 shows the protocol stack for SIP signaling and media.

Fig. 2. Pile de SIP avec les mecanismes de securite

SIP has two categories of entities, users and servers. The user is the User Agent (UA). It transmits and receives communications. Each AU is associated with an identifier called a URI (Uniform Resource Identifier) SIP. SIP URIs is similar to e-mail addresses form, normally containing the user name and domain membership. For servers, there are 4 types:

- Registrar Server: It focuses exclusively on the registration SIP terminals. It receives messages REGISTER. It must identify and authenticate users. It must be connected to a Proxy Server or a Redirect Server that will be in charge of the call.
- Proxy Server: It is used to relay the SIP messages. It plays the role of a server side and client side. It interprets, transforms or translate a message before transferring.
- Redirect Server: It manages call signaling as a Proxy Server, but it does not relay messages. It directly redirects the UA to the required indicating the IP address and port to contact destination address.
- Location Server: it is used by the previous two types of server to obtain information on the various possible locations of a user [8].

SIP messages are divided into three parts:

- The first line.
- The header.
- The body of the message.

The first line is used to identify the type of SIP message and the recipient's address. The header contains information for routing the message as: the reference of the sender, recipient, transaction reference and session security features. Thus the header allows the establishment of a session in terms of location, naming and addressing, but it is the body of the message that describes the media stream set game session. The parameter list of the message body is SDP (Session Description Protocol) format [8].

SIP was inspired by the client / server model particularly prevalent in the world of Internet. Messages are encoded using the syntax of messages HTTP/1.1 [9] and UTF-8 [10]. Exchanged messages are either requests or responses. Textual nature of trade makes it easy to interpret the messages. The association request / response transaction is called. The different possible applications in SIP messages are:

- INVITE: Request to establish a session; inviting a user (human or otherwise) to participate in a telephone or multimedia communication, the issuer of such request y indicates the types of media that is willing and able to receive, in General through an SDP session description (Session Description Protocol) [11].
- ACK Request of acquittal issued to confirm that the sending client a previous INVITE received a final response, the request may carry a session description that ends the negotiation
- BYE Request Closing a call
- CANCEL Request canceled, meaning the server to destroy the context of a call being established (this request has no effect on a call).
OPTIONS this request allows a client to obtain information on the capabilities of a user, without causing the establishment of a session.

- REGISTER request to a SIP server and allows sending the location information (machine where the user is located).

IV. ATTACKS IN THE INTERFACE C-I

The arrival of IMS constitutes the new opportunities attacks in the world of information systems. Signaling and voice sharing the same network and the same technologies as IP data networks, IMS shares the same vulnerabilities as data networks. To this we must be added the risks specific to the signaling and voice transport. We present the different attack was associated to the signaling at the CI interfaces in the following points:

A. The attack by the BYE method

The attacker generates a BYE request and interrupts a conversation. To realize this attack, the attacker listens the traffic and takes the necessary information (such as Call-Id, the From or the To) to generate fraudulent BYE corresponding to the session which is injected into the network. The BYE is not authenticated, who receives the BYE information he executed immediately [12].

B. The attack by the CANCEL method

The attack by the CANCEL method is directed against a client. A third party generates a CANCEL for the establishment of a session. It operates in the same manner as for the BYE attack but this time before the establishment of the session. The server or users think that the appellant canceled. This attack is possible if the user does not authenticate to the REGISTRAR.

C. The attack by the REGISTER method

The attack by the REGISTER method is against the client. By listening to the network an attacker retrieves the identifier of a client. He counterfeit a REGISTER message with the “expires” zero that the REGISTRAR interrupter as deregistration. The customer is not reachable. This attack is possible if the user does not authenticate to the REGISTRAR.

D. Identity fraud

Identity fraud may be the result of low or no authentication. Indeed a SIP proxy can provide a business service session to all requests. Fraudulent calls are attributed abusively to the SIP accounts. Identity fraud can also concern the servers by spoofing the IP address of the latter; illegitimate equipment receives all SIP traffic of the users involved. Without server authentication, the client continues to send SIP requests without knowledge that it dialogue with a pirate device. The attacker can then view the details of all calls and checking it. From that diversion of traffic, the attacker can make denial of service and have knowledge of all the traffic sent by the user. Mutual authentication is need in the context of IMS [12].
shows the principles of operation of the security mechanisms proposed in the SIP RFC and the security solution that proposed by the other research work.

A. Security mechanisms of RFC

The RFC of SIP protocol proposed a stack that includes all protocols that ensures the proper operating of SIP. We develop security mechanisms proposed by this stack.

![Protocol Stack for SIP](image)

**Fig. 6.** the protocol stack for SIP

1) HTTPDigest: HTTP authentication (method "Digest" and "Basic" method) [13] is a based on a challenge / response mechanism. First, it permits the SIP client to register in the REGISTRAR server and then have access to different resources when the server asks it. Authentication is usually required for an INVITE request. The server sends a challenge to the client "nonce", the client responds with a derived "response" value of the challenge and a secret it shares with the server. The server verifies that the client has the same secret by calculating the response in turn and checking the consistency of the two.

2) S/MIME secures a portion of SIP messages using the principle of public key encryption. It ensures the confidentiality, authentication and integrity. Certificates allow either encrypt or sign the SIP messages. Confidentiality and integrity are ensured by the use of the public key of the recipient. Authentication and integrity are assured about them using the private key of the sender. S / MIME in SIP context permits three uses, the transmission of a certificate, the signature and encryption. Encryption of all SIP messages end-to-end needs of confidentiality is not appropriate because of network intermediaries who need to see some field headers to route messages correctly: if intermediaries are excluded security associations, the messages are not routable. Security end-to-end (integrity and confidentiality) is possible for the body of SIP messages, including mutual authentication of users. The "tunnel" mode extends the security header [14].

3) TLS is a modularity protocol which aims to secure exchanges between the client and the server independently of any type of application. TLS acts as an additional layer above of TCP. And TLS is not responsible for reliability Transport Layer or maintaining the connection. The services offered are: authentication, integrity and confidentiality. Its native implementation in many browsers did TLS standard for securing Web applications: HTTPS corresponding to the HTTP association with TLS. Its use is mainly associated with the use of X.509 certificates for server authentication and encryption of trade (i.e. signaling). The initial SIP RFC describing only very briefly the SIP/TLS association [15] was published for the operation of said two protocols. TLS allows the client to authenticate the server. Using a client certificate allow mutual authentication at transport but require the server to have the certificate with the public key of all users: this would complicate significantly the system. In addition, this case is not formally described in [8]

4) IPSec: to protect exchanges in networks, one of the usual solution is to use IPsec (IP security) [16] protocol, the secure version of IP. As SIP provides secure exchanges at the transport layer, it envisages a network level protection with IPSec. This protocol makes it possible to authenticate the origin of IP packets, to ensure the integrity or confidentiality. IPSec therefore protects communications and signaling between two entities. Two modes: transport mode or tunnel mode. Whatever the mode, the SIP server can modify SIP headers and enable the establishment of the call. Generally, SIP clients do not implement this solution. IPSec is mainly used to protect traffic between the two areas.

B. Other research work for securing SIP

1) [17] proposed an authentication mechanism and integrity by adding Integrity_Auth field. The principle of this authentication is based on the pre-shared secret between the client and the supplier. As in HTTP Digest authentication, this solution uses a hash function and a secret to prove the identity of the sender. When receiving a request, the server or SIP client checks the value of Integrity_Auth calculating his own value from the SIP message, the random value and secrecy.

2) [18] Proposes an authentication method using both a password and certificates. The work of [SRI05] explored a solution where the customer does not trade with the SIP Proxy, Proxy for dependents to authenticate the client by exchanging with the Registrar. The servers have certificates issued by an authority.

3) [19] [20] have mainly searched to strengthen the HTTP Digest authentication using a password provided by a third channel. The password for HTTP Digest challenge is provided via a mobile phone. Thus the word of OTP can use safely on a public PC without risk of identity theft.

4) [21] [22] have thus studied how to integrate a SSO solution in the SIP architecture. SAML (Security Assertion Markup Language) is the basis of these proposals. Based on SAML defines an XML protocol for exchanging information related to security, mainly in the SSO applications. [21] is a proposal to integrate SSO solution Liberty Alliance in a SIP environment.
Authentication is provided by centralized server applications all applications. For [22], the SSO server that centralizes applications.

VI. ANALYSIS AND DISCUSSION ABOUT CURRENT SECURITY MECHANISM

The security solutions proposed by RFCs encounter many difficulties in implementation and deployment because encryption of signaling or voice requires a mechanism to distributing secret keys or certificate management infrastructure to be used by all clients or servers. Encryption requires calculation time and increases the size of the IP packet, which is not always acceptable with a real time application such as for the transport of voice for communication. We present the limitations of each mechanism in the following table.

<table>
<thead>
<tr>
<th>Security mechanisms</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPDigest</td>
<td>This method allows dictionary attacks to discover passwords: it suffices to have an association nonce/respons to rebuild the calculation with the method of RFC. More password is short more attack is easy. So it is a method in which only the client authenticates the usurpation of SIP server is possible [24] This solution does not provide any confidentiality.</td>
</tr>
<tr>
<td>S/MIME</td>
<td>One of the major defects of this solution is the absence of infrastructure certificates. It is always possible to exchange certificates with SIP but an attacker can still intercept and modify the S / MIME message. This device also needs to associate each URI a public key that is not necessarily easy. Finally, this solution increases the size of SIP messages.</td>
</tr>
<tr>
<td>TLS</td>
<td>The limits described in the RFC demonstrate that it is difficult to ensure and monitor the implementation of this configuration. Moreover few clients implement SIPS and TLS [25].</td>
</tr>
<tr>
<td>IPSec</td>
<td>In our case, the authentication concerns the voice and signaling flows. It could be envisaged to use IPSec between the client and the server, but it must be an administrator to the configuration: in this case we prefer TLS because the user is free to insert the IMS certificate in his IMS client.</td>
</tr>
</tbody>
</table>

Solutions such as TLS or S/MIME allow protect themselves but require certificate management, which is not common at present in the IMS infrastructure as has already been mentioned. Thus SIP is typically deployed with HTTP Digest authentication in its simple version of a mutual authentication then is now systematic in the new architectures like 3G with AKA [26].

There are many limitations: difficulty to use certificates by absence of PKI interoperability problem, solution related to a choice of protocol in the supports layers (transport or routing level), and difficulty to exchange symmetric keys, absence of political universal Security. This observation leads us to define the following specifications to allow a security solution for SIP signaling appears quickly: do not modify the SIP protocol does not add new fields, strengthen traditional mechanisms present.

The analysis of competing solutions shows that there are two approaches to enhance authentication in a SIP environment. The first solution is to change the syntax of messages, the second to change the architecture and nature of trade. Our logic of changing the generation of certain fields and to define a framework of interpretation can be considered as an innovative way for the security of SIP.

VII. THE SECURITY OF THE REGISTER METHOD IN SIP

In this section we prove in the first step the security problems related to the register method of the SIP protocol in the IMS context. For this we installed a test model to analyze SIP traffic in the C-I interface. This model is composed of the following elements:

- Core IMS with all entities CSCF (Proxy, interrogation and service) and the base HSS, this core is deployed by OpenCoreIMS [27].
- Two routers to transport traffic.
- the Application server
- The IMS client, we used UCTIMC client.

In this platform we started a test registration of client IMS in the IMS core. We capture the results shown in these figures:

REGISTER sip:open-ims.test SIP/2.0
Via: SIP/2.0/UDP 192.168.3.2:5060;port=branch:z9hG4bK1469024095
From: <sip:bob@open-ims.test>;tag=1680565333
To: <sip:bob@open-ims.test>
Call-ID: 754491826
CSeq: 1 REGISTER
Contact: <sip:bob@192.168.3.2:5060;transport=udp;branch=x-v26:5501399904afab>; +sip.instance= "<urn:uuid:9e6056da-6314-11e3-a1d3-97d88ed1e0e4>"
Authorization: Digest username="bob@open-ims.test", realm="open-ims.test", nonce="", uri="sip:open-ims.test", response=""
Server: Sip EXpress router (2.1.0-dev1 OpenIMSCore (i386/linux))
P-Charging-Function-Addresses: ccf=pri_ccf_address
NOTIFY, PUBLISH, MESSAGE, INFO
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE,
Service-Route: <sip:orig@scscf.open-ims.test:6060;lr>
97d88ed1e0e4”

Fig. 10. the request register

REGISTER sip:open-ims.test SIP/2.0
Via: SIP/2.0/UDP 192.168.3.2:5060;port=5060;branch=z9hG4bK1863722346
From: <sip:bob@open-ims.test>;tag=1680655333
To: <sip:bob@open-ims.test>
Call-ID: 754491826
CSeq: 2 REGISTER
Contact:
Authorization: Digest username="bob@open-ims.test", realm="open-ims.test",
nonce="b2ea97ce7e54b65f0c2358e7191a8f55" algorithm=MD5, qop="auth,auth-int"

Content-Length: 0
WWW-Authenticate: Digest realm="open-ims.test", nonce="b2ea97ce7e54b65f0c2358e7191a8f55", uri="sip:open-ims.test",
out_uri=sip:scscf.open-ims.test:6060 via_cnt==3"
req_src_ip=127.0.0.1 req_src_port=5060 in_uri=sip:scscf.open-ims.test:6060
Warning: 392 127.0.0.1:6060 “Noisy feedback tells: pid=25561 result to the proxy.
Please check the input and try again.
Steps 1: The client sends a registration request to the proxy.
Step 2: The proxy responds by sending a random nonce value.
Step 3: The client sends a response derived from secret shared between the client and the proxy and the nonce value.
Step 4: The server responds yes or no if the answer is correct.

These results indicate that the procedure for registering a client passes through these steps:

1. The client sends a registration request to the proxy.
2. The proxy responds by sending a random nonce value.
3. The client sends a response derived from secret shared between the client and the proxy and the nonce value.
4. The server responds yes or no if the answer is correct.

This registration method inherits all the security problems that we develop in this section 4 article. For this we propose to strengthen the SIP register method, by changing the syntax of SIP.

The idea of our approach is to generate a significant value of nonce and not a random value.

In our approach we are looking to generate a nonce value that depends to the following value call-id, realm, URI, secret key and time. So the algorithm we want to realize in the next work is summarized in the following step:

Step 1: The client sends a request for registration which has the following information: call-id, realm, URI and the secret crypt by the public key of proxy
Step 2: The proxy receives the information, it begins in the first step by decrypting the secret by his privat key, in the second step the proxy generate de none by hashing the call-id, realm, URI, secret and time, then send de hashing value to the client.
Step 3: The client receives the value of nonce; he begins by calculating the response bay hashing the nonce and the secret. The client crypt the response value by the public key of the proxy, then send the result to the proxy.
Step 4: Proxy compares the received result with the result calculated by it even. Then send ok or reject to the client.

VIII. CONCLUSION

In this paper, in this work we present a state of art security layer access IMS networks. The work also gives a state of art on the SIP signaling protocol, with different attack related to this protocol in the context of IMS networks. the article develop the current security solutions to secure the SIP protocol, whatsoever the solutions presented in the RFC or the solution in other research work, And provides a detailed analysis about these solutions with a discussion about the limitations of these mechanisms.
We also present a new approach for securing the method registrar in the protocol SIP, because it is present point of all the attack that targets the SIP. The idea of our approach is generate a significant nonce value to ensure mutual authentication between IMS client and the IMS core.

In the future work, we want to model our approach in the modeling tool to testing the feasibility of our solution.