International Journal of Computer Networks and Communications Security

VOL. 5, NO. 4, APRIL 2017, 83–89
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Securing the SIP Communications with XML Security Mechanisms in VoIP Application Awareness

Abdallah Handoura[1], Daniel Bourget[2]

[1, 2] Laboratoire de l'Informatique des Télécommunications, Ecole Nationale Supérieure des Télécommunications de Bretagne France

{[1]abdallah.Handoura, [2]daniel.Bourget}@telecom-bretagne.fr

ABSTRACT

The intelligent network is a basis to establish and commercialize the services by the telecommunication network. Selling services and information by a network does not define solely a considerable increase of the sum of the information flowing by the network, but also a question of confidentiality and integrity. These papers discuss and proposes a methods based on the integration of signaling protocol SIP on IN for realize a procedure of client authentication and data confidentiality.

Keywords: *IN, SIP, threats, security, XML, SOAP, VoIP.*

1 INTRODUCTION

The growing globalization and the liberalization of the market telecommunications, necessitates a more global infrastructure of IN that satisfies needs of different subscribed legal implied, especially for multinational services subscribed. A lot of these services are offered on a current systems, but are often realized with specialists of system. The concepts of IN for given such service is a coherent and stable basis [1]. Some security functions have been introduced already in current systems, but they define constraints to user groups with the private line means, the proprietor equipment and proprietor algorithms or secrets.

There is a major difference between the realization of today service (limited) and the goals of the introduction of IN, however, the IN offer its services to a public world, open, and especially to offer the services that allows user groups of communicate by the public transmission and to change the equipment without unloading their intimacy and affluence of employment.

Therefore, the services of security provide on the current network will not be sufficient for IN, the goal is more long. The defying of the aspect of the new security functions has to make then be publicly usable, economically feasible and insured all its at the same time.

2 THREATS OF THE INTELLIGENT NETWORK

As all elements of a network can be distributed geographically and that elements of system IP are totally opened, several threats of security can rise and attack these different elements. The interconnection IN, is the process to execute a demand of service IN on the part of the user of service through at least two different autonomous areas. Typically, each area represents a system IN separated with different legal entities and entities of resource IN. The limp of the IN service is only to be executed, if the two different areas cooperates by exchanging management, control, and services of data on the basis of a legal contract (co-contract of operation). In this competition, each area applies these clean mechanisms to provide the integrity, the availability, and the intimacy of service user. If the two operators that distribute cooperate, they have to apply the same totality of mechanisms to exchange data between their SCPs and SDPs.

The main problems of security that pose in the multimedia communication area and the telephony over IP as well in a system IN under IP are following:

- Imitation of attack: users not authorized can try to access has services of IN. For example, in the case of service IMR a user not recorded can try to see video services.

- Simulating attack: A recorded user can try to avoid the policy of security and obtains illegitimately access to sensitive services. For example, a user with common access privileges can try to act as an administrator of service IN.
- Denial of Service attack: an adversary can try to block users to access to services IN. For example to send a great number of requests to the system simultaneously
- Communication to spy and alter: an adversary can try to spy and/or to modify the communication between a legitimate user and elements of service IN.
- Lack of responsibility: if IN is not capable to verify the communication between users and its elements of service, then it will not be possible to make that users are responsible for their actions.

The list can be not complete. In practice, nevertheless, one can be found confronted with others problems of security, considered as not belonging of the area of application (for example, problems linked to the policy of security, to the security of management system, to the placement in action of the security, to the security of the implementation, to the operational security or to the processing of security incidents). As well as the technological evolution on the soft, does not cease to increase in a manner not estimable, similarly, the technological connection tools to the system and the attack passive and active become impressive things.

The potential of the threat depends on the implementation of IN, the specific service IN. They depend also on the implementation of security mechanisms (ex. PIN, strong authentication, placement of authentication, management of key, etc).

Manufacturers as well as the groups of standardization make the work of the analysis of risks in the order to improve the security of systems IN. Although a lot of improvements have already been realized, concerning the security of access to SCP and SMP. New services and new architectural concepts necessitate supplementary improvements. The next figure, figure1, presents places of the different threats.

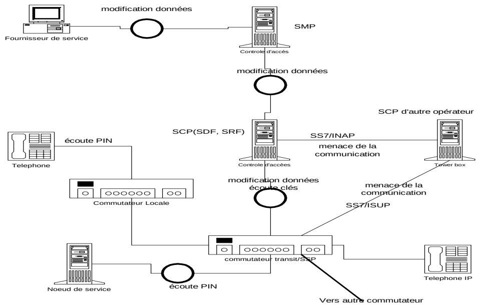

Fig. 1. Places of the different threats.

Intelligent networks are distributed by nature. This distribution is realized not only to the superior level where the services are described as a collection of service feature (SF), but to too low levels, where the functional entities (FE) can be propagated on different physical entities (PE). Like the communications of various elements of network are realized on the open and uncertain environment, the security mechanisms have to be applied.

A responsible of system can prevent these threats of security by using the various mechanisms. The authentication has to be applied in the order to prevent users not authorized to earn the access to the distribution of services.

3 THE SIP PROTOCOL

The SIP protocol (Initiation Session Protocol) is a protocol of signaling to textual structure allows to establish a connection of communication through computer systems between two or several clients by different means (Email, telephone, Web,…) by using the client-server model. SIP employs procedure DNS that allows a client to solve URI SIP in an address IP or port or a protocol of transportation to an other destination to consult [1,2]. SIP message can be encapsulate on different protocol such TCP and UDP. SIP is described as a protocol of control of the application layer. It establishes, modifies and ends conversations. It gathers in syntax of typical HTTP and SMTP (Simple Mail Transfer Protocol) because it allows the establishment of a session between speakers identified by addresses. The SIP transaction demonstrates in the case where a terminal INVITE a second terminal to participate in a new session (modeled by the syntax INVITE). The request emit to a client, who will seek beside a database the information concerning the second terminal. Also SIP Can open canals of communications by textual process or with the help of the voice as it shows the syntax following:

```
INVITE sip: URI SIP/2.0
From:
To:
Call-ID:
CSeq:
Content-Type: application/SDP
v=0
o=
```

4 INTERWORKING BETWEEN INTELLIGENT NETWORK AND SIP

The interest of this integration if it is possible is to profit from different security mechanisms of IP network for Intelligent Network.

The viewpoint IN, elements as SCP, the fact that the request originated from an UAC SIP against a call processing the function on a traditional switch is insignificant. Thus, it is important that the SIP entity is capable to provide the characteristics normally provides by the traditional switch, including the operation as a SSP for IN. The SIP entity would have also to maintain the state of call and to release questions to IN according to services, just as a traditional switch. SIP would have to operate as a SSP. For IN some services necessitating specialized media (such that detection DTMF), or special for the control of call.

SIP does not operate the model of call IN directly for access to services IN, the trick is then to exploit the machine of states of the SIP entity with the layer IN such that the acceptance of call and the router are executed by the native states and the services are accessed to layers IN with the model of call IN [3].

The model of service programming with SIP consists therefore to add on SIP a layer IN that manages the interconnection with the called intelligent system also SIN(Intelligent SIP Network)[3,4]. This operation necessitates the definition of a correspondence between the model of call of IN and the model of call of SIP. A correspondence between the states machine of the SIP protocol (SIP defines the letterhead Record_Route that allows to order SIP to function in mode with states until liberation of the call[5]) and the states machine of IN. A call will be processed by the two machines, the sip machine processes the initiation of call and the final reply deliverance, and the IN layer to act with the node intelligent SCP for providing services during the processing of call [4]. The figure 2 illustrate the integration SIP-IN.

Similarly to the states machine IN, one defines (O-SIP) and (T-SIP), that are the entities correspond, respectively, to the O_BCSM and T_BCSM of the model of call IN.

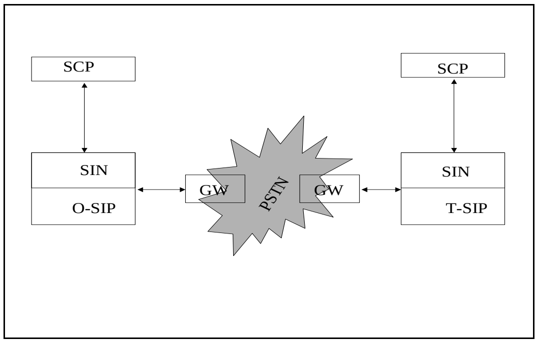

Fig. 2. Interconnection SIP – IN

5 SECURE THE INTELLIGENT NETWORK WITH SIP

SIP Communication is susceptible to several types of attack. The simplest attacks in the SIP permit to assailant of earning the information on users identities, services, media and topology of distribution. This information can be employed and executed others types of attacks. The modification of attack occurs when an assailant intercept the effort and covers the signal and modify the SIP message in the order to change a certain characteristics of service. For example, this sort of attack can be employed for diverted the flow of signaling by forcing a particular itinerary or for changed a recording of user or modifies a profile of service. The sort of attack depends on the type of security (or insecurity) employed (the type of authentication, etc.). These attacks can also be employed for the denial of service.

The main two mechanisms of security employed with SIP: authentication and crypt of data. The authentication of data is employed for authenticate the sender of message and insure that certain information criticizes of message was not modified in the transit. It has to prevent an assailant to modify and/or listen in SIP requests and reply. SIP employ Proxy -Authentication, Proxy - Authorization, authorization, and WWW - Authentication of areas of the letterhead, similar to these of HTTP, for the authentication of the terminal system by means a numerical signature. Rather, proxy-par-proxy authentication can be executed by using protocols of authentication of the transport layer or the network layer such that TLS or IPSEC.

The cryptography of data is employed for insured the confidentiality of communication SIP, allowing only the destined client of deciphered and read data.

It is usual of using algorithms of cryptography such that the DES (DES: Data Encryption Standard) and Advanced AES (AES: Advanced Encryption Standard). SIP endorses two forms of cryptography: end-to-end and hop-by-hop. The end-to-end encryption provides confidentiality for all information (some letterhead and the body of SIP message) that needs to be read by intermediate servers or proxy. The end-to-end encryption is executed by the mechanism S/MIME. On the contrary, the hop-by-hop encryption of whole SIP message can be employed in the order to protect the information that would have to be accessed by intermediate entities, such that letterhead *From, To* and *Via*. The secure of such information prevents malevolent users to determine that calls that, or to access to the information of itinerary. The hop-by-hop encryption can be executed by external security mechanisms to SIP (IPSEC or TLS).

With this technique, an others problem is identified. It is the problem of the assertion and the validation of the identity of user by SIP server. The SIP protocol allows a user to assert its identity by several manners (ex, in the letterhead); but the information of identity requested by the user is not verified in the fundamental SIP operation. On the other hand, an IP client of telephony could have required at insure the identity of a user in order to provide a specific service and/or to condition the type of service to the identity of the user himself. The model of SIP authentication could be a way to obtaining such identity; however, the user agents have not always the necessary information of key to authenticate with all the other agents. A model is proposed in [6] for «confirmed identity» is based on the concept of a «confirmed area». The idea is, that when a user authenticate its clean identity with a proxy, the proxy can share this identity authenticated (the confirmed identity) with all the other proxies in the «confirmed area». A confirmed area is a totality of proxies that have a mutual configuration of security association. Such association of security represents a confidence between proxies. When a proxy in a «confirmed area» authenticates the identity of the author of a message, it adds a new letterhead to the message containing the confirmed identity of the user. A such identity can be employed by all other proxies belonging to the «confirmed area».

Using this mechanism the client UAC, is capable to identify himself to a proxy UAS, to an intermediate proxy or to a registration proxy. Therefore, the SIP authentication is applied only to the communications end-to-end or end-to-proxy; the authentication proxy-by-proxy would have to count on others mechanisms as IPsec or TLS.

The procedure of authentication is executed when the UAS, the proxy intermediate, or the necessary recording proxy for the call of the UAC has to be authenticated before accepted the call, or accepted the recording. In the beginning the UAS sends a request of SIP message «text» (ex, INVITE). In the reception of this message, the UAS, proxy, or proxy of recording decides that the authentication is necessary and sent to the client a specific SIP error message of the request of authentication. This message of error represents a challenge. In the particular case, where the message of error is 401 (Unauthorized) is sent by UAS and recording, while when the message of error is 407 (Proxy Authentication Required) is sent by proxy sever. The UAC receives the message of error, calculates the reply, and includes it in a new message of SIP request. The next figure 3 shows the sequence of message for the case of request of authentication by the proxy server.

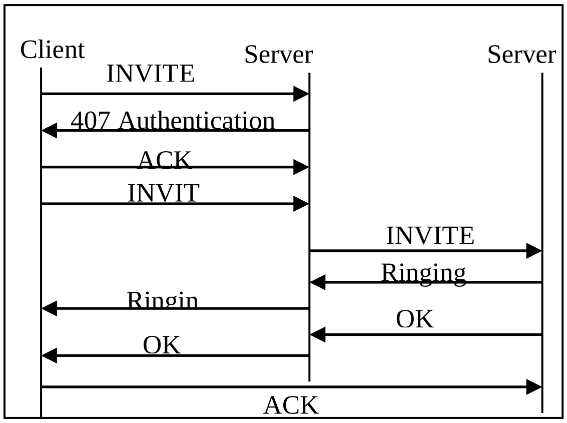

Fig. 3. Authentication SIP

Noting that, the UAC sends a message ACK immediately after that the message of error is received. This message closes the first transaction; then the second message INVITE opens a new transaction.

```
INVITE sip:xy@domain SIP/2.0
Via: SIP/2.0/UDP
To: xy <sip:xy@domain>
From: yx <sip:yx@domain>
Call-ID:
CSeq: 1 INVITE
Contact: <sip:yx@domain>
Content-Type: multipart/signed;boundary=…;
micalg=sha1;protocol=application/pkcs7-
signature
Content-Length:
Content-Type: application/pkcs7-mime;
smime-type=envelopeddata; name=smime.p7m
Content-Disposition:
attachment;handling=required;filename=smime.
p7m
Content-Transfer-Encoding: binary
<envelopedData object encapsulating encrypted
SDP attachment not shown>
Content-Type: application/pkcs7-
signature;name=smime.p7s
Content-Disposition:
attachment;handling=required;filename=smime.
p7s
Content-Transfer-Encoding: binary
<signedData object containing signature not
shown>
```

Fig. 4. S/MIME encryption in SDP

In the use of the mechanism S/MIME, figure 4, it lacks an infrastructure for the utilization of the public key exchange. SIP provides a mechanism of key exchange, but it is susceptible an attack of type man-in-the-middle. To make this, the aggressor can intercept the first exchange of keys between two agents and rest in covers of all dialogues. An other problem of mechanism S/MIME is the difficulty of its configuration to the level user agent.

6 SAOP SECURITY MECHANISMS

6.1 SOAP and SIP

The SOAP protocol allows the transportation of messages coded in XML by the intermediary of HTTP or SMTP in a decentralized and distributed environment. The definition of the SOAP-XML vocabulary and transport protocol HTTP or SMTP is independent. SOAP allows an exchange of information highly flexible and extensible on the independent platforms[8]. It can be also employed not only as a porter of data, but also is that is the most important it is to invoke procedures distanced on servers, services, components and objects write in different languages and distributes on different platforms. It is a norm aimed to simplify the exchange of information by providing a interoperability through a variety of platforms. While SIP can include different data types (acoustics, video or text) based on the Internet protocol that gathers to HTTP, SMTP or IMTP. It is therefore waited that a combination of SIP and SOAP will prove that it is more beneficial when one examines it in the automated agent combination, as opposite agents necessitating the immediate user interaction.

These two protocols define a point of convergence between the Data network and vocal services to the level of the application layer, similarly, a point of convergence between Web and vocal service to the level of the application layer and the SIP protocol.

In this context, we exploiting the combination of SIP-SOAP for profiting of the different techniques of security defined by SOAP for the protocol of signaling SIP.

```
INVITE SIP :
..
Cseq : 1 INVITE
Content-type : test/soap+xml
..
<SOAP-ENV : Envelope>
<user>
</user>
..
</SOAP-ENV : Envelope>
```

Fig. 5. SIP and SOAP

6.2 SOAP security mechanisms

The SOAP Header provides a flexible mechanism for extending a SOAP message. Although the SOAP Header is the best place to add security features to messages, the SOAP specification itself does not specify such header elements.

In general, we have five security requirements for message transmission:

1. Confidentiality guarantees that an eavesdropper can not read the message.
2. Authorization guarantees that the sender is authorized to send a message.
3. Data integrity refers to assurance that the message was not modified accidentally or deliberately in transit.
4. Message origin authentication guarantees that the message was transmitted by a properly identified sender and is not a replay of a previously transmitted message.

5. Non-repudiation guarantees that the sender of the message can not deny that he/she has sent it.

The last three requirements are strongly related to each other. In particular, non-repudiation implies message origin authentication, which also implies data integrity. Data integrity is different from message origin authentication in the sense that the former does not guarantee that the transmitted message is not a replay. In other words, data integrity cannot defend against replay attacks. It is important to note that there is a distinction between message origin authentication and non-repudiation. Keyed-hashing such as HMAC, using a secret key shared in an authenticated way, is sufficient for message origin authentication, but not sufficient for non-repudiation. Non-repudiation requires a digital signature algorithm such as RSA or DSA.
We describe in figure 6 the properties of the SOAP message transmission model and related security requirements.

```
 <SOAP-SEC:Encryption
 xmlns:SOAP-SEC="http://schemas.xmlsoap.org
/soap/ security/">
.....
  </SOAP-SEC:Encryption>

or  Digital signature

<SOAP-SEC:Signature
xmlns:SOAP-
SEC="http://schemas.xmlsoap.org/soap/security/"
.....
 </SOAP-SEC:Signature>
```

Fig. 6. SOAP security mechanisms

The authorization is assured by SIP. The SIP request is:

```
SIP/2.0 407 Proxy Authentication
Required
Via: SIP/2.0/UDP
To: xy <sip:xy@domain>
From: yx <sip:yx@domain>
Call-ID: CSeq: 1 INVITE
Proxy-Authenticate: Digest
Content-type : test/soap+xml
<SOAP-ENV : Envelope>

<SOAP-SEC:Encryption
<SOAP-SEC:Signature
……
</SOAP-SEC:Signature>
</SOAP-SEC:Encryption>
</SOAP-ENV : Envelope>
```

Fig. 7. SIP with SOAP mechanisms security

7 APPLICATION OF THE SECURE IN INTELLIGENT NETWORK FOR VOIP APPLICATION

The service VoIP allows to users connected to a supplier of service Internet (ISP) to realize the calls in PSTN. This scenario to the advantage that the ISP to already a report of security with its client. It is «natural», that the ISP offers this service to the client in addition to the access to Internet. A SIP proxy server in the system ISP will be configured out server band of proxy for client SIP in the system ISP. This proxy sever dispatch of calls to the proxy server of the ITSP (Internet telephony service provider), that will select and contacts the gateways appropriate of SIP.

In this scenario, a possible realization of security mechanism for the calls is as follows: The proxy server ISP employs the proxy authentication procedure of SIP for authenticate the user to call. The ISP authenticates one of its clients. Once the user is authenticated by the proxy server, the proxy verifies if the user is authorized to make a call. If it is the case, the proxy contacts the proxy server ITSP by sending INVITE.

As each system, VoIP is essentially a IP system, VoIP system and terminals suffer of the same threaten inherent with all IP system [7].

The security mechanisms of SOAP are employed for secure the parameters asked for invoke a service beside intelligent systems. Figure 8.

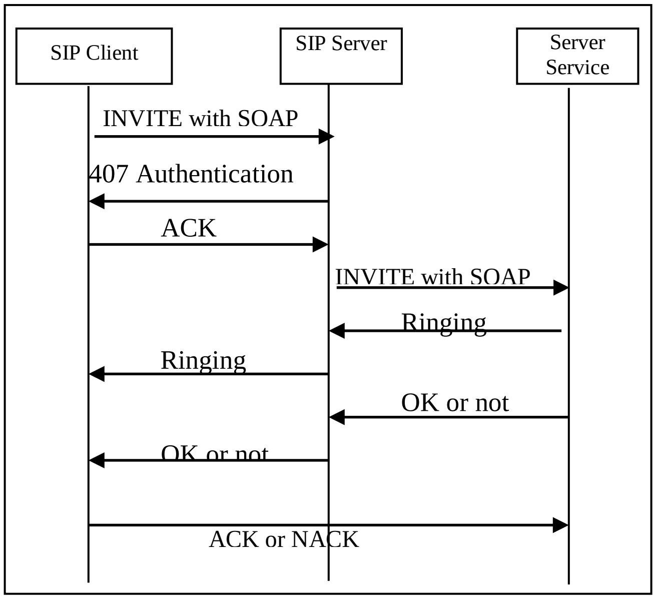

Fig. 8. Intelligent Network security with SIP-OAP(XML).

8 CONCLUSION

With the introduction of intelligent functionality of system on the telecommunication, the necessity for functions of security and the will is emphasized. To integrate the application of this functionality will be the most important, the will give a clear view to each user, that its information's and its orders are processed correctly, and that its information is processed solidly in the system. Of course, there is a long list of functionality demands for services of security, but the main demand list is given by viewpoints of the user. Therefore, in the order to market IN, for the concepts of a technical and economic success, we have to make a good work not only in our laboratory development and in the administration of telecommunications, but also to establish a human comprehension level, political needs and social in our society.

9 REFERENCES

[1] Profos.D "Security requirements and concepts for Intelligents networks" , Ascom Tech AG Bielstrasse 122, 4502 Solthurn.

[2] H. Schulzrinne "The Session Initiation Protocol (SIP)", Columbia University, New York 1998.

[3] VK. Gurbani "Interworking SIP and Intelligent Network (IN) Applications", draft-gurbani-sin-02.txt; June 2002

[4] H. Schulzrinne, L. Slutsman¸ I. Faynberg, H. Lu " Interworking between SIP and INAP", draft-schulzrinne-sin-00.txt; July 2000.

[5] Handoura.A, Bourget.D "Implementing Intelligent Network Services in VoIP application with SIP, TRIP and ENUM", 2nd IEEE International Conference on Information & Communication Technologies: From theory to applications. 24-28 April 2006 Damascus, Syria.

[6] C. Jennings, J. Peterson, and M. Watson,"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", <draft-ietf-sip-asserted-identity-01>, June 2002.

[7] Ranganathan.M.K, Kilmartin.L "Performance analysis of secure session initiation protocol based VoIP networks", Computer Communications 26 (2003) 552–565; 2002 Elsevier Science PII: S0 1 40 -3 66 4 (0 2) 00 1 46 –9.

[8] N. Deason, "SIP for SOAP Sessions", draft-deason-sipping-soap-sessions-00.txt, 23 April 2002.