IJCSN International Journal of Computer Science and Network, Volume 6, Issue 2, April 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

# Securing the SIP Communications with XML Security Mechanisms in Intelligent Network Applications

[1] Handoura Abdallah; [2] Daniel Bourget

[1, 2] Laboratoire Informatique des télécommunications
Ecole Nationale Supérieure des Télécommunications de bretagne – France

**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** - *Intelligent network, threats, Security, XML, SIP, SOAP*

## 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.

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 in 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.

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. 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. Secure the Intelligent Network with SIP

The IN can interconnect with SIP. 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. 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).

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 1 shows the sequence of message for the case of request of authentication by the proxy server.

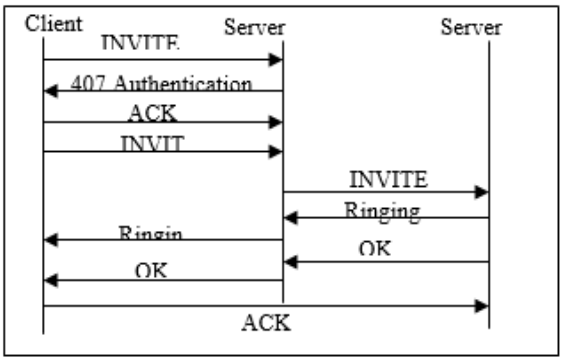


Fig.1 Authentication SIP

In the use of the mechanism S/MIME, 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.

## 4. SAOP Security Mechanisms

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 [9]. 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 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 (figure 2).

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.

The SOAP Header provides a flexible mechanism for extending a SOAP message. In general, we have five security requirements for message transmission: Confidentiality, Authorization, integrity, Message origin authentication and Non-repudiation.

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.

```
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. 2 SIP with SOAP mechanisms security

## 5. Application of the secure in Intelligent Network for multimedia communication

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 3.

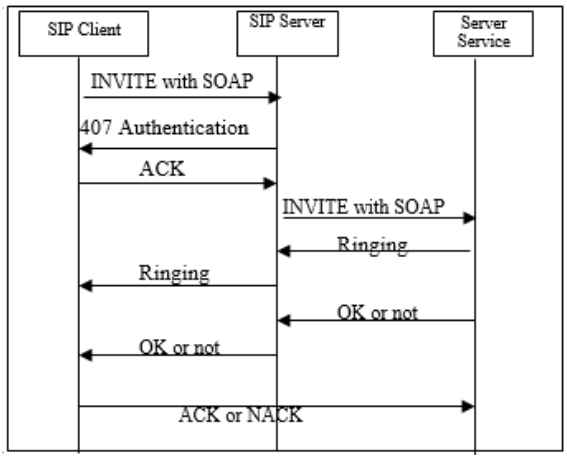


Fig.3 Intelligent Network security with SIP-SOAP(XML)

## 6. 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.

## 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.

[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.

[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] Handoura.A, Bourget.D "Implementing a SIB Intelligent Network with VoiceXML, SIP and Web services", 2006 IEEE International Conference on System of Systems Engineering: Control, Command, Communication, Computing and Information; Los Angeles 24-26 April 2006.

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