The security of web services: Secure communication and identity management

Hasnae L'AMRANI [#1], Younès EL BOUZEKRI EL IDRISSI [#2], Rachida AJHOUN [#3]

[#] *Higher National School of Computer Science and Systems Analysis (ENSIAS), University Mohamed V, Morocco*

[1] hasnae90lamranii@gmail.com

[3] r.ajhoun@um5s.net.ma

[#] *National School of Applied Sciences of Kenitra (ENSAK), University Ibn Tofail, Morocco*

[2] y.elbouzekri@gmail.com

***Abstract*— Service Oriented Architectures have become the new trend in the world of communication on the web. Especially web services are the high-performance specification of service-oriented architectures. The use of confidential data on the Web becomes the primary problem in the secure communication over the web. The solution proposed in this paper is a secure communication tool OCS based on the principals of SAML standard and Single Sign-On.** **Our solution proposes a new approach which collaborates strong points of SAML standard and single sign-on method. The implementation of this approach is in the form of a platform or a tool which provide a secure communication between web services. Thus, a future approach that exceeds the level of authentication and address the level of access control, likewise and as a further step, prepare an evaluation of the most important technologies which provide Single Sign-On possibility and secure communication context between heterogeneous web services.**

Keywords: SOA - web services – SAML – SSO – secured communication – security tokens - Secure communication tool on the web (OCS) - Shibboleth.

I. Introduction

Currently, online banking exchange, sending confidential email, online trade, the exchange of government information on networks is all at risk network uses. For these reasons, the secured exchange on networks is becoming more necessary than ever. Certainly the use of secure protocols can guarantee a level of confidentiality, message integrity and user authentication, but this level still minimal compared to the value of the information exchanged over the network. For this, the stress of communication between all web services, distributed over a network, while maintaining the diversity of domains and flexibility of data exchange need a deeper discussion about mechanisms for authentication, and secure communication over a network considered vulnerable.

The procedure of authentication, based SSO protocol (Single Sign-On) could solve the problem of domain change, and re-authenticate with every area of change (Cross-Domain) required for distributed applications. Furthermore, the combination of SSO with the secure exchange of confidential data, and a good identity management can improve safety communications in web services.

The most important objectives of this work are:

- Establish the state of art on the actual service oriented architecture situation, especially, web services security issues.
- Treat authentication problems and detect the major problems of communication between web services.
- Investigate on web services security standards as much as analyze identity management systems and their most significant models, not only that, but also single sign on authentication method.
- Prepare an appropriate study about SAML standard as it is treat authentication level, also do the same with single sign-on method.
- Propose a new approach which collaborates strong point of SAML standard and single sign-on method. The implementation of this approach is in the form of a platform or a tool which provide a secure communication between web services.

In what follows, we will see all concepts related to service-oriented architectures, web services, subsequently the security of web services and in particular, the standards for the safety of web services, SAML standard as a technology for a securities exchange , Single Sign-On and finally we will present our approach entitled secure communication tool (OCS).

II. SERVICE ORIENTED ARCHITECTURES AND WEB SERVICES

There are various ways to define a Service Oriented Architecture. The majority of these definitions focuses on the technical aspects of SOA, although others show business characteristics. SOA is an architecture style that allows the reorganization of the information system. It enables the encapsulation of an information system functionality into a loosely coupled service belonging to both a business and technical levels of the company [1].

Web services are modular applications that can be made, published, located, and invoked automatically in a web. Thus, applications can make use of features located on other machines in other applications. In the end, we can say that the original purpose of a Web service is to make possible the use of an application component in a distributed way.

III. WEB SERVICES SECURITY

In recent years, under the impulse of major participants like IBM and Microsoft, some work aims to fill gaps of web services security. Some of the evolutions of these actors, creation and investment in the field of standardization and standardization results agreed on standards for web services security. There is a usual of standards for the security of web services and identity management models.

A. The standard of web services security

A standard is a repository published by a private entity other than a national or international standards body or not approved by one of these organizations for a national or international standard [2].

Many standards and recommendations have been developed in the field of security of web services. IBM and Microsoft have prepared the documents describing the technical strategy and roadmap for integrating security architecture based on web services security.

Developed standards concern the establishment of a trust network, the definition of security policies, and implementation of access control... [3].

<table>
<tr><td>WS-Secure Conversation</td><td>WS-Federation</td><td>WS-Authorization</td><td rowspan="2">XACML</td></tr>
<tr><td>WS-Security Policy</td><td>WS-Trust</td><td>WS-Privacy</td></tr>
<tr><td colspan="3">WS-Security</td><td>SAML</td></tr>
<tr><td colspan="2">XML-Encryption</td><td colspan="2">XML-Digital Signature</td></tr>
</table>

Figure 1: standard of web services security

The figure identifies security standards of web services that we present some of them:

SAML Standard:

SAML standard (Security Assertion Markup Language) V2.0 [4] was designed by OASIS as a framework for the exchange and propagation of safety information between trusted partners. The security information's are expressed as assertions about entities with an identity in the security domain. Assertions can provide information on the attributes of the features on authentication already made or authorization decisions related to specific resources [5].

XACML Standard:

XACML defines a language for the formulation of access control policies. It specifies the necessary features for the treatment of these policies and a data flow model of the functional components for the infrastructure. XACML provides authorization mechanisms that are transferred by SAML standard in other words XACML complement SAML to provide the authorization service.

WS-Trust Standard:

WS-Trust is based on the WS-Security security mechanisms and defines a model for the establishment and maintain trusted relationships across security domains. In service-oriented architectures, confidence usually involves the emission, exchange and validation of security tokens to control access for specific services.

WS-SecureConversation Standard:

WS-SecureConversation standard allows a secure communication and a confidential communication. It uses public key for the exchange session keys and specifies the mechanisms for establishing and sharing security contexts. This protocol associated with the application level is the equivalent of SSL at the transport level [3].

B. Identity management models

To address the problem of multiple user accounts for each service used, and the great effort of memorizing passwords for these accounts, different identity management models was developed. The notion of identity management requires an ensemble of models to meet the requirements interested organizations:

model	Description
isolated model	In this model, each service provider (FS) has the responsibility for managing the identity of each of its users. FS deploys its own identity management system (IMS) taking into account the complexity and functionality defined by the organization. It is very difficult for FS, to integrate these IMS to provide coordinated services [7].
centralized model	This model is based on the single storage of digital identities. The user can authenticate with all service providers using the same identity [7].
federated model	In the federated model, the saved identities in different service providers are linked through pseudonyms. The entities that make up the federation form a Circle of Trust (CC) establishing trust relationships [7].
User-centric model	This model has been designed to give users more control over their personal data. Indeed, they can select the identity provider that suits them and choose the identity to use to access the different services [7].

Table 1: A different identity management models

IV. Secure communication and single sign-on

Before beginning the concept of single sign-on and the secure communication, it is necessary to say that our goal is to see the usefulness of the combination of these two important climbed in terms of improving the web service security.

A. *Single Sign-On (SSO) :*

The Single Sign-On is a process that allows a user to authenticate once to access multiple applications or resources.

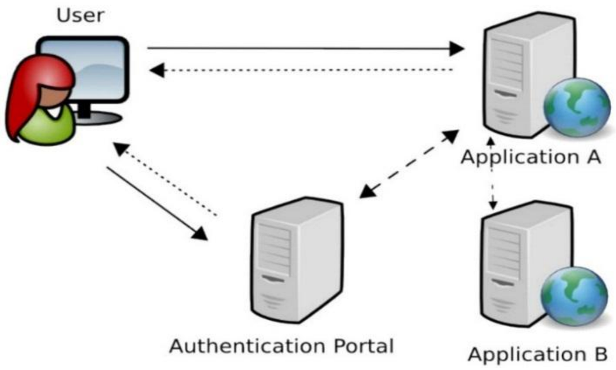

Figure 2: architecture of SSO

This is a simplified model of single sign-on that shows the radical principle of it. We note that the user may have access to all the resources of both applications. A single authentication guarantee repeated access to the resources.

B. *Secure communication based on SAML*

In this contribution, we were choosing to focus our work on authentication level and as we explained above, SAML standard has treated authentication problems by securing the message's contents. For those reasons, we will explain in details Security Assertion Markup Language standard.

So, communication between different remote services, concern for safety, plays an important role in the design of strong and effective safety standards.

SAML standard, namely Security Assertion Markup Language, is dedicated to helping developers for making security contexts over the application-level for the communications based on computers or between security domains. In this function SAML standard transfer authentication data that take care of terminal capacity to protect against illegitimate uses systems.

For the parts of SAML standard standards are illustrated in the diagram below:

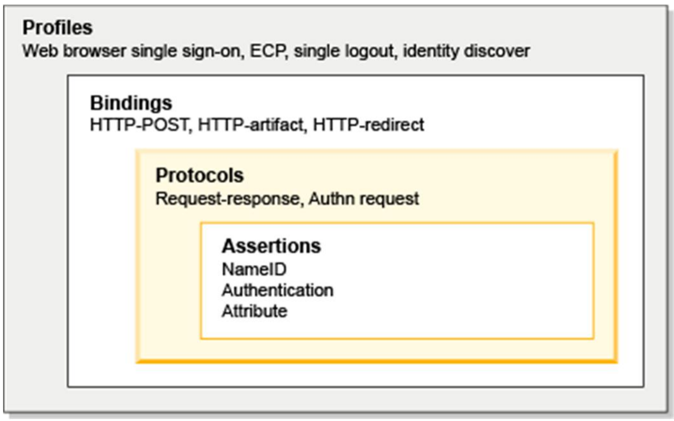
Profiles
Web browser single sign-on, ECP, single logout, identity discover
Bindings
HTTP-POST, HTTP-artifact, HTTP-redirect
Protocols
Request-response, Authn request
Assertions
NameID
Authentication
Attribute

Figure 3: SAML components

SAML standard is used for secure information exchange between business partners online. SAML manages the information needed to authenticate and exchange processes between partners. These exchanges are based on assertions, protocols, bindings and SAML standard profiles.

V. The secure communication Tool : OCS

After studying single sign-on and SAML standard, we have proposed a solution which is based on these two technologies. This solution is a tool that allows secure communication between web services. Also, it ensures single sign-on between different services.

A. *Functional principle*

A tool for Secure Communications (OCS) brings together the strengths of these technologies point, this tool allows a demand and supply of services in a secure way. The figure below explains the general principle of operation of the proposed tool.

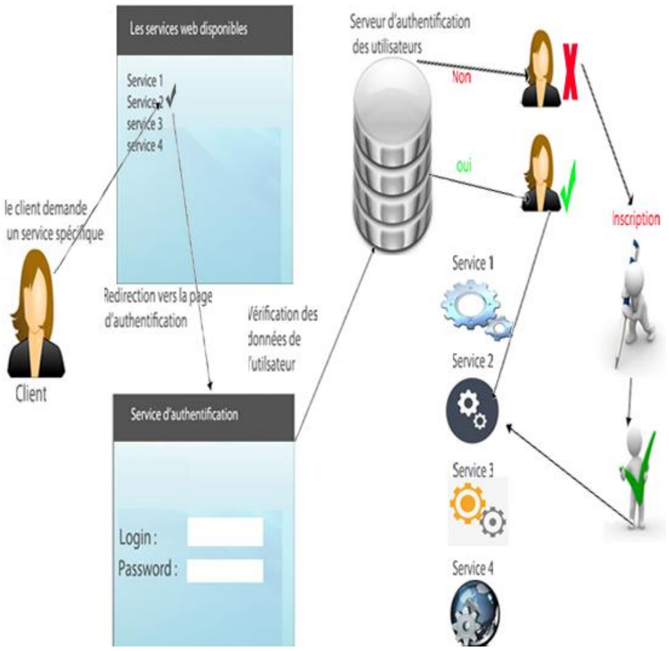
Les services web disponibles
Service 1
Service 2
service 3
service 4
le client demande un service spécifique
Client
Redirection vers la page d'authentification
Vérification des données de l'utilisateur
Service d'authentification
Login :
Password :
Serveur d'authentification des utilisateurs
Non
oui
Inscription
Service 1
Service 2
Service 3
Service 4

Figure 4: Principle of functioning of the proposed tool

The user before reaching the desired service passes through a series of steps to finally get to use it. The steps in this process are divided as follows:

- Service Request; ;
- Redirect authentication;
- Checking the user account;
- Redirection to the desired service;
- Registration of new users;
- Validation of new users;
- Redirect requested service;

B. *Implementation*

The establishment of a practical solution, developed by ourselves was our goal. The developed tool provides a roadmap for users who want to access the web services by keeping the confidentiality of their private data. Web services developers can take this tool as a starting Framework, and then simultaneously enrich and improve its level of security. In what below, we will explain how we had implemented our approach and give more details about every step mentioned above.

OCS tool is a framework based JEE language and contain a list of web services distributed on different applications. Our tool provides the following processes to access and manipulate web service functionalities.

Service Request:

User request one of the services provided on the web services portal, he must to choice one of those services and send his request.

Redirect authentication:

After Service Request step, the user is redirected to the authentication portal where he can log in for reach the access to the service demanded.

Checking the user account;

When the user's credentials are received, we check if this user is identified in our Identity Provider or not, else according to their situation he will be redirected to these services wanted or to the inscription portal.

Redirection to the desired service:

The user who had the appropriate privilege is directly redirected to resources requested, and he can access to other services in a secure way, because this passage from one service to another is based on security tokens.

Registration of new users:

The user who is not registered in our Identity provider must continue the registration process, then we will evaluate his account and, after that, we will decide to validate or reject his inscription.

Validation of new users;

Actually, the administrator is the one who validates or reject the user's inscription and he can also disable some account temporarily.

Redirect requested service;

When the new user account is valid, he will be directly redirected to the service which he requested, and commence to have the same privileges of the old users.

The table below presents the objectives achieved and not achieved after the development of the SCO tool:

Objectives	Satisfied	Unsatisfied
Secure communication between web services based Tokens	yes	
Transparent transition between the different web services available	yes	
Encryption passwords in the database	yes	
Centralized authentication in the identity provider	yes	
Single Sign-On based on security Tokens	yes	
Sends of authentication data for the first		Not yet

connection on a secure way		

Table 2: Assessment of satisfaction for OCS tool

This evaluation isn’t a fixed point of view, it supports a lot of modifications, however, our tool is still in the amelioration and we continue to supply it with news ideas and propositions.

VI. Future work

The establishment of a secure communication between the service and its users is a very complicated mission. In order to achieve the success, it should not stop at a minimum safety level, moreover, looking for other more effective solutions.

In this paper, we examined the SSO technology and the SAML standard, thereafter we developed a tool for secure communication (OCS) which is inspired by those two technologies.

All the results achieved stops at the authentication level; either by keeping the safe passage for the private information (SAML), or by using single a sign-on (SSO). For all of this and as a perspective, we propose to expand the circle of research at the management of the access control.

In order to achieve this goal, we plan to investigate in identity federation technology “Shibboleth” more thoroughly and compare it with other technologies like OpenID, OAuth...

Identity federation, single sign-on systems (SSO), the connection and the disconnection in the SSO systems will be our future main research lines.

Finally, we contemplate to compare our tool (OCS) with other tools such as: shibboleth, OpenID…, to locate the strength and weakness not just of our proposal but also of the other technologies.

VII. Conclusion

The study of security standards for web services and their areas of intervention and systems identities management have enriched our scientific research about web services security. The extensive studies on the safety standard SAML, components, operation and threats that target has improved our knowledge of the safe transfer of data authentication and authorization on the web. In addition, the SSO brought another level of security for web services, by reducing the number of authentications, and subsequently decrease the probability of interception of private user data.

The proposal of the "OCS" tool is an innovative step, because it reflects secure connections between clients and services trade. This tool provides a secure authentication and communication between the client and the web service and then have a secure communication context procedure. As an outlook, adding a distribution server for a security tokens temporary, specific to each user for each service will be our goal to prevent attacks like session hijacking and other attacks targeting private customer data.

References

[1] «Interconnexion des processus Interentreprises : une approche orientée services».

[2] «http://fr.wikipedia.org/wiki/Norme_et_standard_techniques#Standard,» [En ligne].

[3] P. B. Nassar, «Gestion de la sécurité dans une infrastructure de services dynamique : Une approche par gestion des risques,» 2012.

[4] U. i. d. t.-S. D. L. N. D. L'UIT, «Langage de balisage d'assertion de sécurité (SAML2.0)». Brevet X.1141, 13 juin 2006.

[5] M. E. Hughes J., «Security Assertion Markup Language (SAML) V2. 0,» OASIS SSTC Working Draft, 2005.

[6] M. U. FRAGOSO-RODRIGUEZ, «Modèle de Respect de la Vie Privée dans une Architecture d(identié fédérée,» 16 décembre 2009.

[7] P. B. Nassar, «Gestion de la sécurité dans une infrastructure de services dynamique : Une approche par gestion des risques,» 2012.

[8] C. B. e. x. L. G. G. L. Maesano, Services Web en J2EE & .NET conception et implémentation, paris: ÉDITIONS EYROLLES 61, bd Saint-Germain 75240 Paris Cedex 05, 2003.

[9] G. HARRY, «IAM : GESTION DES IDENTITES ET DES ACCES CONCEPTS ET ETATS DE L’ART,» 12 Septembre 2013..

[10] G. Zhenhua, «Research and Implementation of a SAML-based SSO module,» Institute of Network technology, Beijing University of Posts and Telecommunications, beging, 21 Décembre 2012.