Assuring Security and Privacy for Extensible Access Control in Open Web Services by using Finger Print Identification

S. Nirmala Sugirtha Rajini
Research Scholar,
Dr.MGR. Educational Research Institute,
Chennai.

T. Bhuvaneswari
PhD, Assistant Professor,
Government Arts and Science College,
Bargur.

ABSTRACT

In recent years, web services have become a new application over the open, complex internet. In that, web services security issues have become more and more important. But, there is no effective access control method to assure the web service security. This paper proposes a simple and effective formalization of concepts that have to be supported for enforcing the new access control model needed in open scenarios, towards the aim of providing a solution actually deployable with today's technology. Finally our frame work addresses privacy and trust issues, and authorization policies protected resources whose access is subject to credential proof and trust level validation to enable access control interactions between web service clients and servers by using image processing techniques.

Keywords

Web services, interoperability, Policy Decision Point (PDP), Policy Information Point (PIP), Access Control, minutiae point

1. INTRODUCTION

Over the last few years, web services and the service-oriented architecture (SOA) have become main themes in IT across many industries. Web Services (WS) are considered one of the main technologies which provides an application in integration technology that allows business applications to communicate and cooperate over the internet[6]. Web-based computing, service orientation, and cloud computing increasingly displace the client/server approach.

Web service security is an open standard that specifies how security related meta-data should be incorporated into SOAP (Simple Object Access Protocol) messages. Web service security does however, does not define security models, mechanisms or technologies but rather defines how existing approaches should be applied to SOAP messages to ensure interoperability among different implementations and languages. For that purpose, web service security defines several basic elements for the SOAP headers to hold security information [3].

To enable the seamless interoperation between web services, security policy intersection aims to provide a security policy that will satisfy both the service provider and consumer [2]. Nowadays many organizations share sensitive services through open network systems and this raises the need for an authorization framework because the servers generally do not have prior knowledge of the requesters. However, these attributes may themselves be considered sensitive and so may need protection from disclosure. To overcome this problem we can provide an extension to XACML (eXtensible Access Control Markup Language-novel concepts) that enables clients and servers which establish it as the rising technological solution for controlling access in an interoperable and flexible way. Although supporting the most common policy representation mechanisms and having acquired a significant spread in the research community and the industry.

2. PROPOSED ARCHITECTURE

To access the information from the open web services the following architecture is proposed.

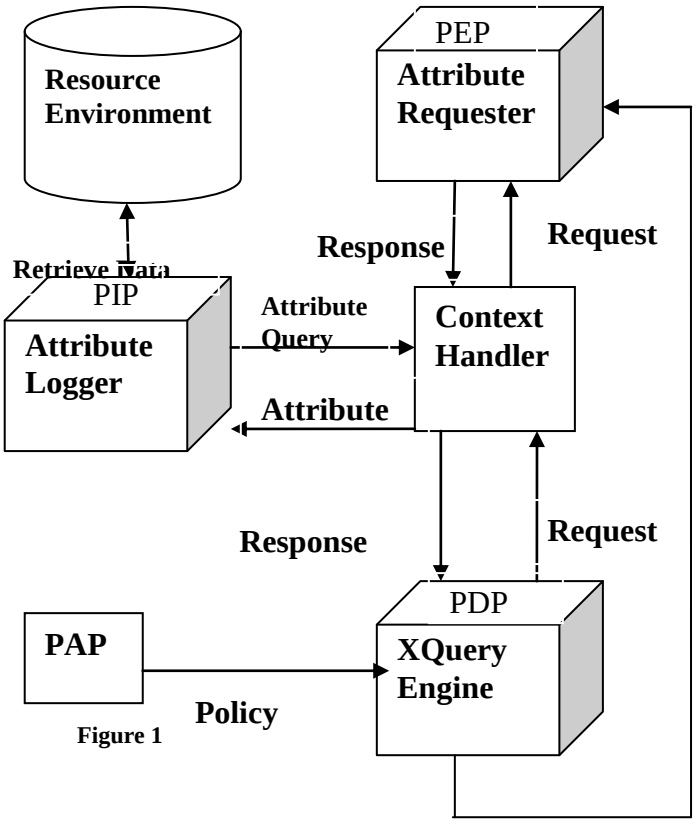

Figure 1

PAP - Policy Administration Point
PEP - Policy Enforcement Point
PDP - Policy Decision Point
PIP - Policy Information Point

The requester sends an access request to the PEP module, which has to enforce the access decision that will be taken by the PDP. The requester has to release all relevant information for policy evaluation. The PEP module sends the access request to the Context Handler that translates the original request into a canonical format, called XACML request context, and sends it to the PDP.

The PDP identifies the applicable policies by means of the PAP module and retrieves the required attributes and, possibly, the resource by means of the Context Handler. The context handler also relies on the PIP module to access attribute values about the subject, resource, action, and environment. To this purpose, the PIP interacts with the Subject, Resource, and Environment modules. The Environment module provides a set of attributes that are relevant to take an access decision and are independent from a particular subject, resource, or action.

The PDP evaluates the policies and returns the XACML response context, together with an optional set of obligations, to the Context Handler. The Context Handler translates the XACML response context to the native format of the PEP and returns it to the PEP. If some information is missing, the PDP cannot take a decision and returns an error (Indeterminate response). The PEP fulfills the obligations and, if permitted, it gives access to the requester. Otherwise, access is denied. Based upon this architecture the user can access the overview information about the particular open web service. To access the entire information from the web service we can propose a new image processing approach for security.

3. PROPOSED METHODOLOGY

Here, to view the entire information of the service the user should register with the web server by providing the finger print in order to know the user. During the access time after verifying the username and password the current user name is compared with the stored finger print data.

Our image processing approach is mainly based on the minutiae-based representation of a fingerprint. In which the fingerprint is represented by two minutiae feature parameters: 1) x and y coordinate of the minutia point 2) i.e. the minutia orientation. Our approach gives the number of matched minutiae on the basis of these features by considering reference fingerprints and uses it to generate similarity scores[4]. According to forensic guidelines, when two fingerprints have a minimum of 12 matched minutiae they are considered to have come from the same fingerprint . So more matched minutiae yield higher similarity scores. When the number of minutiae on both fingerprints is less than 12 then the access denied information is displayed otherwise the entire information will be displayed to the user.

4. ADVANTAGES OF PROPOSED METHODOLOGY

The proposed methodology is capable of finding the correspondences between minutiae without resorting to exhaustive research and this methodology also provides more security than other security algorithms because every person's finger prints are different from each other. In addition, since the minutiae based fingerprint representation is standard and widely used in the most existing fingerprint databases.

5. CONCLUSION

The existing architecture still suffers from some limitations which affect its ability to support actual requirements of open web-based systems. The unauthorized user is also able to view the entire information. The previous open service authentication techniques are used by giving only the user name and password for identifying the user. To maintain the dialog management and to view the entire information and for the user access of server knowledge we have to go for some new authentication technique which is proposed. After finger print verification only, it displays the entire information. In future, we will implement the privacy and trust issues to view the entire information of the service; the user should register with the web server by providing the finger print in order to know about the user. Hence we will use any one of the image processing algorithm to compare the fingerprints.

6. REFERENCES

[1] Claudio A. Ardagna, Sabrina De Capitani di Vimercati, Member, IEEE, Stefano Paraboschi, Eros Pedrini, Pierangela Samarati, Senior Member, IEEE, and Mario Verdicchio, June 2011. Expressive and Deployable Access Control in Open Web Service Applications" "Web Services Security Policy Assertion Trade-offs

[2] Lavarack, T. Coetzee, M. Acad. of Comput. Sci. & Software Eng., Univ. of Johannesburg, Gauteng, South Africa , 2011. Web Services Security Policy Assertion Trade-offs

[3] Stefan D¨urbeck, Christoph Fritsch, G¨unther Pernul and Rolf Schillinger Department of Information Systems University of Regensburg, 2010. A Semantic Security Architecture for Web Services – the Access-eGov Solution

[4] Ashwini R. Patil Mukesh A. Zaveri, Sardar Vallabhbhai, 2010. A Novel Approach for Fingerprint Matching using Minutiae".

[5] Lavanya B N, K B Raja, Venugopal K R and L M Patnaik, 2009 Minutiae Extraction in Fingerprint using Gabor Filter Enhancement

[6] Sawsan Abu-Taleb and Hossam Mustafa, 2010 Improving Web Services Security Model.

[7] Mohsen Ghazvini, Hiwa Sufikarimi, Karim Mohammadi Fingerprint Matching Using Genetic Algorithm and Triangle Descriptors.

[8] Gorrell Cheek, Mohamed Shehab, Truong Ung, Ebonie Williams 2011. iLayer: Toward an Application Access Control Framework for Content Management Systems

[9] L.R. Palmer, M.S. Al-Tarawneh, S.S. Dlay and W.L. Woo 2008 Efficient Fingerprint Feature Extraction: Algorithm and Performance Evaluation

[10] Mitsuo Okada Yasuo Okabe, Tetsutaro Uehara, 2009. Security Analysis on Privacy-Secure Image Trading Framework Using Blind Watermarking.