Improving the Security of a Networking Semantic Service Oriented Architecture.

E. STERGIOU[1], S. V. MARGARITI[1]
[1]Department of Teleinformatics and Management
A.T.E.I. of Epirus
GR-47100 Arta
GREECE

D. C. VASILIADIS[1,2], G. E. RIZOS[1,2]
[2]Department of Computer Science and Technology
University of Peloponnese
GR-22100 Tripolis
GREECE

Abstract: - The Semantic Web is expected to change the way of Enterprises' operation. This study is focused on a novel secure structure relating in an efficient networking service-oriented architecture for delivering secure Semantic Web Services. It is presented initially all the technical factors (e.g. the associated protocols) and explained the networking architecture. The proposed issues for an appropriate secure infrastructure using a networking service-oriented architecture defines a set of security requirements. Hence, we introduce a proper set of definitions for delivering more efficient and secure Semantic Web Services on an intranet, or even on the Internet. Using those novel definitions the services will be able to have more flexible and secure access via the Web. Furthermore, we deal with the associated lookups, where Semantic Web Service-oriented architecture imposes specific requirements onto the corresponding lookup service. According to our proposal, all authentication issues can be properly implemented using the Lightweight Directory Access Protocol by two alternative (direct and indirect) methods. Finally, this paper aims to act as a point of departure for future studies on how Service-oriented architecture can be used to improve the security and the functionality of the Semantic Web Services.

KeyWords: - Semantic Web, SOAP, XML, Security, Semantic Web service, LDAP.

1 Introduction

The new Web will change of operations of Enterprises. At the next years the Web services are forecasted to have a progressive transformation to new generation web. The new generation Web which Tim Berners-Lee and others [1-2] called "Semantic Web", is an extension of the Word Wide Web. The Semantic Web Service will still contribute in the diffusion of more information in internet, and it will increase our dependence from this. The Parsia etc [3], presents a semantically-aware policy language by translating WS-Policy into OWL-DL. As it is known the Web Ontology Language (OWL) is a W3C standard for defining semantically rich language. The OWL Description Logic (OWL-DL), is a subset of OWL that guarantees completeness and decidability. The L. Qin etc [4], presents an access control model for Semantic Web. They insist that their access control is capable of specifying authorizations over concepts defined in Ontologies and enforcing them upon data instances annotated by the concepts. This Semantic web aims at machine-possible information. In this paper, we propose a set of new security definitions for an efficient Service-oriented architecture. In addition to, we use a novel authentication way using the Lightweight Access Protocol.

This paper is organized as follows. Section 2, presents the architecture of a Semantic Web Service, explaining the protocols and basic elements. Section 3, presents an integrated security structure as requirements for a secure web application. Section 4, explains briefly the accessibility through the Lightweight Access Protocol. In section 5, the security of the SOAP protocol is analyzed and a novel authentication method presented using the Lightweight Access Protocol in access control. Finally, Section 6 provides the concluding remarks.

2 Architecture of Semantic web.

The new Web Service is a combination of programs and methods making the Data Bases accessible and available through the Web pages in a secure manner. This new coming Web Service will allows programmers (as a third party) to have easy access in DB through the Internet. The various existing Data Bases is not essential to have homogeneity from each other. In any case all the DBs, will be exploited by Web Service. The semantic web technology deals with data processing and transferring. The main elements of new Web Service are:

1) The XML Language. 2) The transfer protocol SOAP. 3) The search service UDDI. 4) The description Language WSDL.
All the above main elements, which support the new Web Service are briefly analyzed in the following subsections.

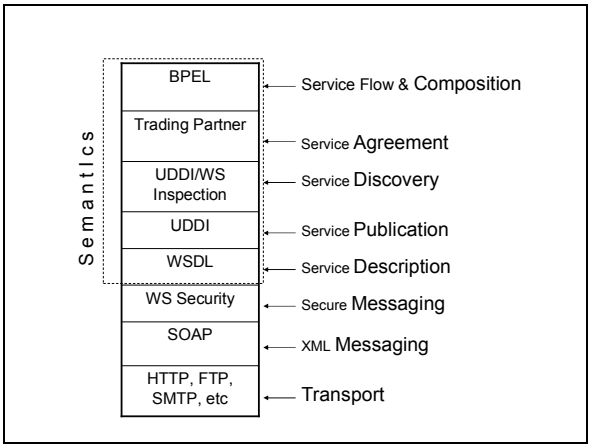

Fig. 1 Semantic Web Service Stack.

Fig. 1 depicts the Semantic Web Service Stack.

2.1 The XML Language in the Web Service.

The XML Language is a global language for data presentation. The programs that are based on XML Language – have high interoperability. This Language use text, in order to present data, so the bulk of data, is low.
The data from the XML Layout are received by specific fields. As far as, the information of the XML fields are matching with corresponding fields of the Data Bases, then data might be exported from these Data Bases, and those data can be transferred into Web pages. Furthermore, by similar way, Data Bases can be compared each other, if two or more Data Bases have equivalent fields, e.g. the *price* with field "price" and the *quantity* with field "quantity", etc.

2.2. Protocol SOAP.

Because the new Web service supports Web applications with interoperability, is necessary to have a mechanism which will transfer the given XML data fast through the Internet. This mechanism implemented by the SOAP (Simple Object Access Protocol).
The SOAP Model was invented in order to bridge XML pages with HTML pages in comprehensible way. Using SOAP is ensured the "behind" compatibility. That means, all the data that could be transported by HTTP protocol, can be transported by SOAP protocol as well, without any problem. The SOAP Protocol acts as a general "wrapping" that it helps in the dispatch of data in binary form. It operates as an envelope. The SOAP does not know what exists inside but it can be recognized. Thus, data become acceptable from the Web Servers through the Browsers.
Consequently, a new Web service application can be written by any programmer who is able to combine the use of the XML Language, the SOAP protocol and data from "open" Data Bases.

2.3 The search service UDDI.

The model UDDI (Universal Discovery, Description, and Integration), allows to the Web Service applications to search the Data Bases, with the same way as the Google searches the Web pages. In order to achieve this, the UDDI creates and holds the UDDI registries. The UDDI registries are the main elements for the various Data Bases, which are be "opened" in the WWW. At the infrastructure level, UDDI is a standard registry that stores taxonomical descriptions [6] of Web services.

2.4 Description Language WSDL.

According to what mentioned before the basic idea is to exploit the "opening" Data Base in the Internet. We can do this, rather easily, with the use of WSDL (Web Services Description Language). The WSDL is another new element which comes to supplement the new generation of Web Service. The WSDL covers the need of automatic notification of services or elements of Data Bases etc.

Only few text lines will be enough to make a notification to Internet for the basic elements of a Data Base. This WSDL service allows in a machine to calculate, what needs a site as soon as it has a WSDL text. A program that has access in a Web Service recovers a description WSDL from this Web service. The description is special XML data that inform the user with the processes that can use and provide data for each process.

The combination of UDDI and WSDL is a combination that works much better from a person which is involved the finding and evaluation of elements of Data Base in the WWW. Using the New Web Service, will not be needed a person to seek information using Engines Machines.

2.5 The Semantic Web.

Let's consider two machines in the Internet which will be able to communicate between each other. Nowadays, in order to achieve this, is necessary to have an agreement between two communicated parts about the data structure that can be used. On the

other hand, in the Semantic Web, it is not needed any agreement between two communicated parts. This connection between documents and notions is achieved by Ontology. The Ontologies are the groups of data that build the semantic Web, and from these groups extracted the visions of the semantic web. The Ontology's syntax is a set of rules or models which follow the words, when the words are combined in proposals.
The semantic of a web makes many elements in an entity. An entity-ontology element – can be considering as a set of RDF statements. The group of RDF elements determines various relations between the elements of application and also determines reasonable effects between each other.

The Semantic Web allows to the software agents to 'understand' Data Bases. The Web pages that are coded in XML language, and the RDFs, determines the structure and the attributes of Data Bases.

The Semantic Web is a machine for reasoning. The approach of the World will not become in mechanistic way as it becomes today but via reasoning.

3. Web Service Security.

The Semantic Web is a set of decidable subset of OWL and Conditions with Markup Language. In the next text we present, a set of novel security definitions in modules integrating the security of SOA. These definitions can be considered as general guidelines in development of SOA.

3.1 Security Definitions for SOA.

As explained in above, the new WWW is expected to be flooded by XML transported data. However the XML data is ASCII code which is also easily can be malicious. It means that it is necessary to have additional actions by a secure mechanism in order to support the transportation of data in a safe manner. Up to today the problem of Safety has not been solved. There are many scenarios for this. For example, a proposal is focus on the use of encryption methods by the two parts.

So far many proposals for cryptography, consider the usage of Cryptosystem with public key may be a good method. The usage of GM-security (also called polynomial security) is a suitable method for security. According to the [7] the GM-security (also called polynomial security) and the semantic security is much more similar (or equivalent). This solution considering as not so satisfy, because of the delay that be presented in the transferring data.

Another proposed solution is, the usage of the SSL transport protocol which is also used today and it is very common. However and this protocol is characterized as a "heavy" protocol. At the end up today, doesn't exist any specific significant solution for security and this maybe is a gap for the integration of new Web service.

The security must be satisfies the following basic aims. First, only one appropriate interaction between parties that take place at any time must exist. Second, before the system being in interaction mode, the parties under question should be able to verify their security requirements and capabilities with other clients. During this verification in the case of conflicts, suitable mechanisms must resolve them. Third, the security of SOA must be facing the needs of Clients and the needs of system administrators. The Clients needs flexibility whereas on the other hand the system administrators prefer restricted policies.

A Secure agent based system should have to satisfy the following general points:

1) Authentication mechanism to allow the mutual authentication mechanism. This mechanism must allow the authentication of agent and agent platforms verifying their identities by each other.

2) Authorization, in order to allow agents to have access to the platform resources.

3) Data integration and confidentiality during transmission.

We consider that systems will be secure only if satisfy all the above criteria. The systems will be rather fair if satisfy some of the above criteria and on the other hand the systems will be bad if doesn't achieve to satisfy all the above criteria.

In order to evaluate the security, we introduce a set of criteria that can be used in order to make safe a system.

3.1.1 Definition for Knowledge Base.

In OWL there is a definition of Knowledge Base that is be used for authorization. The OWL, OWL-DL, must be used to represent the information. This Knowledge Base must have a description of end points of the network. This Knowledge Base must describe all the information that needed by the Client who wants to make authorization.

3.1.2 Definition for Access Control.

Theses definition used in order to define the access rights of Clients to the information represented in

the knowledge base. The Semantic Web Rule Language (SWRL) is a set of decidable OWL and Rule Markup Language. Those definitions must be written in a semantically familiar language. If we use SWRL we are able to provide support in complex relationships between properties. If we use SWRL the results is much better than the usage of OWL-DL. The Definitions for Access Control may be written in the manner of protecting the access of two specific resources, the web service endpoints and the information that comes back.

3.1.3 Definitions for Evaluation.

If definitions for Knowledge Base and Authorization rules are written in OWL-DL, this OWL-DL element must be used for evaluation the Rules.

3.1.4 Definition for Authorization.

The Authorization decisions must be made with relevant Web Service End Point. The result of the Authorization can be in full access mode or in limited access mode or without access mode. In case of limited access mode, the Clients have the ability to access part of the information. Clients may be able discover web site that fulfill their requirements, but they can not be able to access the service because they don't have the relevant rights. Another possibility of rejecting access is the use of incompatible security mechanisms.

3.1.5 Definition for Secure Semantic Device.

In the context of having more secure services, we introduce a relevant semantic device that can operate as a Firewall. This kind of device can be used properly by a system administrator for sending and receiving messages implementing efficient security policies. This device may support all the above definitions and requirements. It is also important to build a secure ontology to describe security concepts and creating tools that use semantic annotation of security. However, the Ontologies may need to be expanded or to include additional elements for example *trust* and *QoS*.

All the above special Secure networking Definitions, gives a flexibility and easy way to manipulate the security elements without confusing. We must keep in our mind, all these definitions, during the building of Semantic Web Service applications.

4. Accessibility and LDAP Directory.

LDAP provides directory access mechanism that allows globally distributed information to be stored uniquely in a database. The LDAP composed of two main sections.

One section will be the network protocol standardization. And the other section indicates the structure of the directory schema. Typically, the information is stored in a tree structure, like a management information base schema. Every entry has a unique Distinguished Name (DN). Given a base DN, we can use a Relative Distinguished Name for an entry with a pre-defined base directory tree. The following example shows an entry with a unique DN:

cn=elef ster, os= NETWORKING SUBSECTION, ou= TELEINFORMATICS DEPARTMENT, o=ATEI of EPIRUS, c=EUROPE

where: *cn*- common name, *os*- organization subsection, *ou*- organization unit, *o*-organization and *c*- Continental.

The most important action of the LDAP takes place on the directory access. The central purpose of a directory service is to enable people or programs to search for information, thus the search request message is an important LDAP operation. The LDAP protocol structure enables a client to send requests to a directory and receive responses, in a simple way. In LDAP, there are several different types of requests. In order to retrieve the content being stored in a LDAP database, we can follow the LDAP URL and URI setup to inform a remote LDAP server from to search for a database entry. With the DAP URL and URI, we can use web browser to enable LDAP commands.

5. Authentication Method and SOAP.

The SOAP is a protocol for invoking methods on servers, services, components and other objects in Semantic Web Applications. There is a set of methods in order to have secure exchange SOAP messages. The security elements can be embodied in SOAP messages or can be acquired from external services by following Security Token Reference [9]. This security tokens can be retrieved and registered with existing access methods. Our proposal consists of the usage of LDAP and XKMS [5] standards. Both of them provide a web service client which lacks direct access to the security tokens with an offloading mechanism.

5.1 Secure SOAP messages through LDAP.

The Web Service retrieves the security tokens stored in a directory through LDAP as a security token access method. Here we explain the operation of access token for a SOAP message. It is assumed that the Web service provider needs to contact the Security Token Service in order to fetch and verify its security token. In Fig.2 pictured a General Structure of *Web Service Request and Response* with Security Token Reference.

In the following steps explained the operation of Web Service Request.

Step 1: The clients who request a service build a

SOAP message. The structure of this message is like the Fig.2. As can be seen there is the *signature* elements denoted as: *<ds:signature>*, and inside in this section there are two sub-sections: the *<Security Token Reference>*, and *<ds:KeyInfo>*. The *Security Token Reference*, reference to the external token or the certificate. The *KeyInfo* sub-section referred to the X.509 Token or Token ID. The Token ID, is denoted in the previous *Security Token Reference* sub-section.

Step 2: The above constructed message is sent to the Web Service.

*Step 3:*The Web Service fetches *KeyInfo* sub-section. In order to retrieve the certificate, the Web service will send an LDAP request corresponding to the reference URI. The *Security Token Service* searches for the certificate according to the LDAP URI (this paragraph is embodied in the Client's Web Service Request).

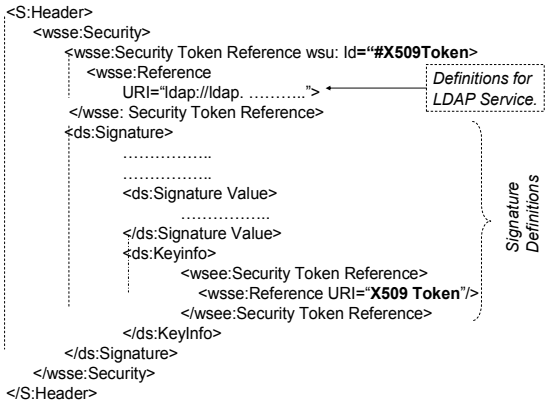

Figure 2 General Structure of Semantic *Web Service Request and Response* with Security Token Reference.

The Token Service returns the resulting certificate as a result. The Web Service provider validates the *<wsse:Security>* in the *Signature* sub-section and processes the SOAP message to return the service result. The LDAP, attribute and assertion values are represented in octet string.

5.2 Secure SOAP messages through XMKS.

Another way to have validation is using the PKI architecture. When a PKI is used for Semantic Web Service we can have two types of PKI clients. One case when we have directly access to PKI, and the other indirectly access using service proxy like XML Key Management Specification (XKML) Service [5], which provide clients with a well defined interface to a PKI. Figure 3 illustrates a general PKI architecture which is comprised of CA, SA end entities.

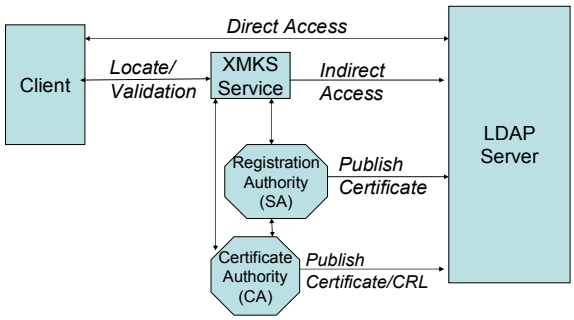

Figure 3 Direct and Indirect invoke to LDAP Service.

There is a corresponding to Fig. 2, *Locate Service Request* that used for integrate the access through the XMKS and the LDAP.

6. Conclusion.

The growing use of Web Services will affect vitally the way of operation in enterprises, organizations and the society. The demand for secure issues raises the number of difficulties, relating both to the complexity of the interactions and to the development of appropriate protocols for supporting those interactions.

Especially, in this paper a novel scenario is analyzed which gives some considerable challenges in the development of SOA relating to an appropriate security infrastructure. We propose some novel definitions about the security structure and policies for SOA.

Furthermore, two specific authentication schemes are presented using the LDAP Directory server. We expect this novel proposal to make the Semantic Service architecture more flexible and secure to be certificated accessible.

All the above proposed components and the whole security structure are needed to be tested comprehensively in order to have more efficient and secure systems.

References:

[1] Tim Berners-Lee, Weaving the Web, Harper, San Francisco, 1999.

[2] Tim Berners-Lee, James Handler, and and Ora Lassila, "The Semantic Web", Scientific American, May 2001.

[3] B. Parsia, V. Kolozski and J. Hendler, Expressing WS Policies in OWL. 14th International World Wide Web Conference, Chiba, Japan, 2005.

[4] L. Qin and V. Atluri, Concept-Level Access for the Semantic Web. ACM Workshop on XML Security, Fairfax, VA, USA,2003.
[5] W3C. XML key management specification (XKMS) W3C Standard, March 2001.
[6] UDDI Spec Technical Committee. UDDI Version 3.0.2., OASIS 2004, available on line at http://uddi.org/pubs/uddi_v3.htm.
[7] Yevgeniy Dodis, Matthias Ruhl. GM-Security and Semantic Security Revisited, MIT Laboratory for Computer Science, 1999
[8] Haarslev, V. and Moller, R. 2001. Descriptionof the RACER System and its Application. In Goble, C. A.; McGuinness, D.L.; Moller, r.; and Patel-Schneider, P.F., eds., Working Notes of the 2001 International Descriptions Logic Workshop (DL-2001), volume 49 of CEUR Workshop Proceedings.
[9] OASIS. Web service security: SOAP message security 1.0 (WS-Security 2004). OASIS Standard 200401, March 2004.