Role Based and Credentials Based Access Control in Semantic Web

Shaily Malik
Lecturer, CSE Dept. Maharaja Surajmal Instt. of Technology Janakpuri, New Delhi-110058
Email: shaily.singh99@gmail.com

ABSTRACT
Semantic Web is the new generation web which is also known as the “Web of Meaning”. The services provided by the semantic web have enabled the World Wide Web to "understand" and satisfy the requests of people. The different layers of Semantic Access Control Model (SAC) use the metadata to understand the semantics of the different elements relevant for the access decision. Access Control is one of the prime issues that are to be taken care by any network. Access to the systems and resources should be controlled in a much safer way[4]. The semantic web should have some access control mechanism so that only the authorized users are able to access the data. This paper presents an approach to enable access control for semantic web services and then show how concept-level security policies can be represented in an OWL-based access control language[1].

KEYWORDS
Semantic web, Access control

1. INTRODUCTION
Semantic web is nothing without the web services. Semantic web ontologies describe the web services in a more understandable form. It provides intelligent, autonomous and adaptive agents for the upcoming infrastructures like grid computing, invasive computing and web services. There are three Issues that threaten the security in semantic web: access control, data mining methods and trust negotiation techniques[4]. Access Control is one of the prime issues that are to be taken care of by any network. Access to the systems and resources should be controlled in a much safer way. In this paper we present an access control model that addresses the problem of semantic integration of external authorization entities in the applications and to provide a dispersed and scalable framework supporting advanced authorization and access control schemes in an efficient way[2].

2. LAYERS OF THE SAC MODEL
The essentials of Semantic Access Control as shown in Figure 1 are the description of numerous metadata models, described in the following subsections, at different layers of the semantic web. Each section of SAC represents the semantic model of a component of the access control system. Semantic dimensions enclosed in that meta models are used for the specification of access control criteria, dynamic policy allocation, parameter instantiation and policy validation processes [3]. On one hand, SPL access control policies take advantage of the different metadata models (Policy, PAS and SRR) for its creation and syntactic validation (Structure level). Moreover, these models are vital for the semantic and appropriate validation of the policies, because they facilitate us to perform supposition processes and formal validation of the SPL specifications [7].

2.1 Access Control
Access Control is one of the prime issues that are to be taken care by any network. Access to the systems and resources should be controlled in a much safer way. The semantic web should have some access control mechanism so that only the authorized users are able to access the data. This paper presents an approach to enable access control for semantic web services and then show how concept-level security policies can be represented in an OWL(Web Ontology Language)-based access control language[3].

In this paper we present an access control model that addresses the problem of semantic integration of external authorization entities in the applications and to provide a dispersed and scalable framework supporting advanced authorization and access control schemes in an efficient way[5].

2.1.1 Need Of Access Control In Semantic Web:
2.1.1.1 The end user should be able to prove his/her authenticity for a web service or collection of web services with the help of some framework.
2.1.1.2 The structure must sustain the specification of complex access control requirements. The access control requirements of a Web service may depend on the requested functionality which is controlled by the input parameters.
2.1.1.3 The framework used should be able to identify the interaction between the access control and the functionality of Web Services. The Web Services are of two type: Atomic and
Composite. An atomic Web service which is not decomposable into parts. On the other hand the composite Web services can be broken into parts and known as component Web services. A Composite Web service consists of data flow graph and a control flow graph that shows that how the data is flowing and how the component Web services are connected into a set of Web services.

2.1.1.4 The Web service provider is responsible for computing the access control policy of a composite Web service. So we need a framework to support it.

2.1.1.5 A framework is required to take into consideration the number of credentials that are issued to the requester at the time of execution of a composite Web service.

2.1.2 ACCESS MECHANISMS

When bearing in mind the security necessities of many distributed applications, authorization frequently comes forth as a central element in the design of the whole security system because of authorization is the source of the trust chain. Some of such characteristics are flexibility, heterogeneity, interoperability, dynamism, mandatory access control, role based access control. The role based access control is usually considered a mature and flexible technology. Some of the access control schemes are discussed below:

2.1.2.1 Role based access control

Computer systems have shown multiple applications and assisted multiple users, that has lead to sensitive vigilance of data security issues. System administrators and software developers focused on different kinds of access control to ensure that only authorized users were given access to certain resources or data. One access control mechanism that emerged is role-based access control (RBAC). A role is mainly a semantic construct forming the basis of access control method. Along with the RBAC scheme, system administrators create roles according to the job functions performed in a given environment, grant permissions (access authorization) to those roles, and then assign users to the roles on the basis of their specific job responsibilities and qualifications. A role can represent specific task competency, such as that of a physician or a pharmacist. Or it can embody the authority and responsibility of, say, a project supervisor. Roles define both the specific individuals allowed to access resources and the extent to which resources are accessed. For example, an operator role might access all computer resources but not change access permissions; a security-officer role might change permissions but have no access to resources; and an auditor role might access only audit trails. Roles are used for system administration in such network operating systems as Novell's NetWare and Microsoft's Windows NT. This article explains why RBAC is receiving renewed attention as a method of security administration and review, describes a framework of four reference models the authors have developed to better understand RBAC and categorize different implementations, and discusses the use of RBAC to manage itself. The authors' framework classifies the administration of RBAC from its access control affairs. The use of OWL (Web Ontology Language) to define policies has several very significant advantages that turn out to be decisive in distributed environments involving coordination across multiple organizations. First, most policy languages define constraints over classes of targets, objects, actions and other constraints.

2.1.2.2 Credentials based access control

Credentials are the digitally signed documents that can be broadcasted by committed channels like Web. Credentials emphasize a fastening between a principal and some property. A principal represents a user and depending on the perspective recognized by her public or clandestine key. The significance of declared assets may be a arranged capacity for a service, an identity or a non-identifying attribute of a user. The credential-based public key communications SPKI/SDSI(Simple Public Key Infrastructure/ Simple Distributed Security Infrastructure) grants each principal to issue credentials. SPKI, SDI and the other certificate mechanisms from 1996 onward started out to address apparent over complication in the X.509 world. SPKI/SDSI requires no central certification authority. Unlike other public key infrastructures. So, any Web service provider is able to issue and trust credentials independent of other service providers and even give their own trust structure. A Web service provider, acting as a verifier, can locally and separately decide whether access to her service should be contracted or not. Depending upon the SPKI/SDSI certificate assigned to any user the access decisions are made. It is also possible that the users can request for a specific Web service spontaneously without registering themselves with the individual Web service providers. So we can say that the credentials based access control method is better than the classical authentication based schemes that we used for Semantic Web.

3. CONCLUSION

The main objective of semantic web is to enable computers and people to work in cooperation. A necessity for this is encoding data in forms that make web contents more comprehensible by algorithmic ways. This paper presents two types of access control schemes for protecting Semantic Web resources. The semantic approach of semantic access control is the basis to accomplish semantic interoperability among the different components of access control systems. The semantic access control reaches the highest layers of the Semantic Web (Logical, Inference and Trust). To enhance the expressiveness of the model for describing the authorization rules, more expressive logics in logic layer of Semantic Web stack can be applied. This paper showed how credentials can be used in the Semantic Web and how SPKI/SDSI can be used to specify credentials.

4. FUTURE SCOPE

The research can be carry forward on development of additional semantic models to enable secure delegation of attribute certificates.

Continued on Page No. 84
5. REFERENCES


[9].