ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 6, No. 3, 2011, *pp*. 177-194

Ontology-Based Access Control Model for Semantic Web Services

A. Mohammad [1], G. Kanaan [2], T. Khdour [3], S. Bani-Ahmad [4]

[1]The Arab academy for Banking and financial sciences, Damascus, Syria.
[2]The Arab academy for Banking and financial sciences, Amman, Jordan
[3,4] Al-Balqa Applied University, Salt, Jordan

(*Received March 7, 2011, accepted March 20, 2011*)

Abstract. Studies show that reducing the gap between security services and semantic web is important. In this paper we present an ontology-based access-control (OBAC) to support semantic web service. For that, security ontologies are developed to specify concepts and terms involved in this model. Our proposed access control model is expressive and general with these important features: (i) The use of ontology provides reasoning ability for access control decision making, and allows access control information to be automatically searched, queried and discovered. (ii) Our proposed model has a higher degree of interoperability compared to other approaches of access control mechanism. This is because of the nature of ontologies in providing semantic interoperability. (iii) Our proposed model is context sensitive; the constraint ontology represents different types of context constraint. (iv) Our proposed model is designed based on the widely accepted semantic web languages, Web Ontology Language (OWL) and Web Ontology Language for Service (OWL-S), therefore its implementation can be easily achieved by using already existing tools designed for working with these languages.

1. Introduction.

"The Semantic Web is not a separate Web but an extension of the current one, in which information is given well defined meaning, better enabling computers and people to work in cooperation. " (Berners-Lee et al., 2001). The functioning of the Semantic Web will depend on a number of technologies. Some important ones include XML, RDF and ontologies figure 1. Semantic Web services is an essential part of the Semantic Web development, it's vision is to describe Web services' capabilities and content in an unambiguous, computer-interpretable language and improve the quality and robustness of existing tasks such as Web service discovery and invocation (Mcilraith et al., 2001), bringing semantic to security services especially to access control play an important role in the integration between semantic web and security service, this integration in his turn play a major role in facilitating automatic reasoning for access control of Semantic Web services, The boom of the Internet led to the creation of ontology languages for exploiting the characteristics of the Web, Such languages are usually called Web-based ontology languages or ontology markup languages, From all of them, the ones that are being actively supported are now RDF, RDF Schema, ontology web language (OWL), and ontology web language for services (OWL-S) which was developed in the context of the work on Semantic Web Services, OWL-S defines an upper ontology for describing the properties and capabilities of Web services in OWL. It is intended to enable users and software agents to automatically discover, invoke, compose, and monitor Web resources offering services, under specified constraints, hoverer the shift from current Web to semantic aware environments such as the Semantic Web poses new security challenges especially in the field of access control. Access to web services on the Semantic Web can not be controlled in a safe way unless the access decision takes into account all the factors such as context constraints, heterogeneous of subjects and resources and automation of role assignment, Traditional access control models like MAC, DAC and RBAC fail to address these issues since they need to be accommodate to dynamic, open and distributed web service environment and then to be compatible with

[1] *E-mail address*: abdulgahfour@yahoo. com
[2] *E-mail address*: ghkanaan@aabfs. org
[3] *E-mail address*: khdour_thaer@hotmail. com
[4] *E-mail address*: sulieman@case. edu

the semantic web. in this paper our proposed access control takes into account all of the issues and utilize the web ontology language for services (OWL-S) to be compatible with semantic web, semantic web service (e. g. defined by OWL-S) is represented as process which has input, output, preconditions and effects, in this process, we introduce the semantic access control model as a condition figure 3, So In this paper, we present the ontology-based Access Control model (OBAC) which is an extension, or in other word an ontology representation to Context Sensitive Attribute and Task- Role Based Access Control (CSAT-RBAC) for web service application which utilize the characteristics of Role Based Access Control Model (RBAC), Attribute Based Access Control Model(ABAC) and Task Based Access Control Model(TBAC), however CSAT-RBAC has several considerable features that make it a suitable access control model for Semantic Web services, for example CSAT-RBAC is capable of handling dynamic and anonymous users and reducing security management tasks. CSAT-RBAC also supports a wide range of access control policies and provides fine-grained access control for Web service applications such as controlling parameters of the user request. However, the aim of this paper is to develop a semantically compatible access control model for Semantic Web services by providing ontological representations for the concepts and relations involved in the CSAT-RBAC model, each component of CSAT-RBAC is represented in a separate ontology such as credential ontology(on behave of subject), web service ontology (the protected resource), session ontology, constraint ontology, permission-role assignment ontology, user-role assignment ontology, and then we could integrate these separate ontologies to get the complete access control ontology which plays the role of a condition in semantic web service process. This will allow security services to be integrated with Semantic Web services. Such integration will facilitate automatic reasoning for access control of Semantic Web services.

The reminder of this paper is as follows; in Section 2 we discuss the preliminaries relevant to the Semantic Web. Section 3describes the related works on this topic, and section 4 states the fundamentals of OBAC by applying the ontology techniques to describe the access control model components (Each component of ERBAC will be defined in a separate ontology), the complete ontology-based access control introduced in section 5, Our proposed architecture for implementing the ontology-based access control(OBAC) model is presented in section 6 Finally, section 7 underlines some conclusions and future research lines.

2. Background

2.1. Semantic Web and Ontology

The aim of the Semantic Web initiative is to advance the state of the current Web through the use of semantics. More specifically, it proposes to use semantic annotations to describe the meaning of certain parts of Web information and, increasingly, the meaning of message elements employed by Web Services. For example, the Web site of a hotel could be suitably annotated to distinguish between the hotel name, location, category, number of rooms, available services and so forth. Such meta-data could facilitate the automated processing of the information on the Web site, thus making it accessible to machines and not primarily to human users, as it is the case today. The current web standard for semantic annotations is RDF and RDF Schema, and its extension OWL. Suitable annotations are useful for improving the accuracy of Web searches. The search engines can look for pages in which precise concepts from ontology are marked instead of collecting all pages in which certain, generally ambiguous, keywords occur. But the vision of the Semantic Web cannot be achieved solely by disambiguating and relating individual concepts. At least equally important is the integration or transformation of data structure elements. Besides some platform specific parts, data structures reflect in a contracted and simplified way how the designer perceives the possible states of affairs of the respective application. Ontologies allow for the formal specification of an application domain that can be shared by different systems. For instance, one system may distinguish hotels from guest houses. Another only refers to accommodation in general. Location may be given in coordinates, in metric distances or in walking distances to relevant fix points. Ontologies allow intelligent systems for mediating between these different forms to organize information. This ability constitutes a major prerequisite for the global access to Web services. A particularly interesting application of ontologies is the seamless integration of services, information systems and databases containing general knowledge. For instance, an ontology combining kinds of geographic units, kinds of tourist services and their relationships could be used to determine that Crete is an island in Greece, and therefore a Greek island and Heraklion a city on Crete. It would further describe that accommodations are immobile, and that hotels are kinds of accommodation. Such information would be crucial to establish a connection between a requester looking for accommodation on a Greek island, and a hotel advertisement specifying Heraklion as the hotel location (Grigoris et al., 2007).