Chapter 14
Semantic Mapping for Access Control Model

Yi Zhao
Lehrgebiet Informationstechnik, Germany

Wolfgang A. Halang
Lehrgebiet Informationstechnik, Germany

ABSTRACT

With the increasing development of the Semantic Web technologies, the Semantic Web has been introduced to apply in the Web Services to integrate data across different applications. For the Semantic Web Services to succeed it is essential to maintain the security of the organizations involved. Security is a crucial concern for commercial and mission critical applications in Web-based environments. To guarantee the security of the Web Services, security measures must be considered to protect against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Access control is a kind of security measurements to guarantee the service processes, which is defined to allow resource owners to define, manage, and enforce the access conditions for each resource. In this chapter, an attribute based access control model with semantic mapping (SABAC, for short) is proposed to specify access control over attributes defined in domain ontologies. The model is built on the basis of XACML policy language. Semantic mapping process is proved to be syntactical, semantic, and structural. Our SABAC model between the service requester and service provider can make the access to the Semantic Web Services secure.

1. INTRODUCTION

With the increasing development of the Semantic Web technologies and the increasing need for information systems integration in organizations, the Semantic Web has been introduced to apply in the Web Services to help integrate data across different applications, which causes a security problem. Hence, for the Semantic Web Services

DOI: 10.4018/978-1-60960-765-4.ch014

to succeed it is essential to maintain the security of the organizations involved.

Security is a crucial concern for commercial and mission critical applications in Web-based environments. To guarantee the security of the Web Services, security measures must be considered to protect against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Access control is a kind of security measurements to guarantee the service processes, which is defined as the mechanism that allows resource owners to define, manage, and enforce the access conditions for each resource (Samarati, 2001). Up to now, there are a lot of access control models have been proposed such as the mandatory access control (MAC), the discretionary access control (DAC), role-based access control (RBAC) (Sandhu, 2000), attribute-based access control (ABAC) (Priebe, 2004), and context-based access control (CBAC) (Corradi, 2004). A major drawback of the approaches mentioned above is that they do not exploit the rich semantic interrelationships in the data model. The relative complement is the semantic-aware access control model which contains semantic-based access control (SBAC) (Javanmardi, 2006), and semantic context-aware access control (SCAC) (Ko, 2008). These two models support making more precise decisions regarding authorization and inference rules. They fetch users' context and ontology from middleware, with which context hierarchies are built. However, the semantic relationships between the contexts, authorizations and inference rules are not considered.

Web Services are defined as small units of functionality, which are made available by service providers for use in larger applications. The intention to develop Web Services was to reduce the overhead needed to integrate functionality from multiple providers. However, extensive human interaction is still required in the process. Semantically enabled Web Services are forming the research area known as Semantic Web Services (SWS) (Payne, 2004). Semantic Web Services are kind of Web Services whose descriptions are annotated by machine-interpretable ontologies, so that other software agents can use them without having any prior knowledge about how to invoke them. Since Web Services are mainly designed for the purpose of integration of different applications and platforms, it is very important to find a convenient access control mechanism which can interoperate easily with any information system.

In this chapter, an attribute based access control model with semantic mapping (SABAC, for short) is proposed to specify access control over concepts defined in ontologies. The model is built on the basis of XACML (Moses, 2005) policy language with the application of semantic mapping. The semantic mapping is realized between the attributes of the service requester and the service provider. The mapping result can be kept in a mapping base for reuse, and similarly, the generated access control policies can be saved for future reuse. All of these can make the access to the Semantic Web Services secure.

The whole chapter is organized as follows. The preliminaries relevant to the Semantic Web, ontology, Semantic Web Services, access control models, as well as the architecture of the XACML model, are given in Section 2. In Section 3, some currently used Semantic Web based access control approaches are investigated, and the motivation of our access control model is presented; The architecture of the proposed semantic mapping based access control model SABAC, and its performance principle which includes the semantic mapping method, the policy reuse are also described in Section 3. Section 4 gives the authors' some future research work. Section 5 concludes this paper.

2. BACKGROUND

The Semantic Web (Berners-Lee, 2001) is a universal medium to exchange data, information and knowledge. It suggests annotating web resources with machine-processable metadata. The emerg-

Innovation in the Time of Pandemic: Insights from a Survey of Malaysian Small and Medium Enterprises (SMEs)
Mohammed Alnajjar, Abdelhak Senadjki, Au Yong Hui Neeand Samuel Ogbeibu (2025). *International Journal of SME Research and Innovation (pp. 1-21).*
www.irma-international.org/article/innovation-in-the-time-of-pandemic/368040