ABSTRACT

This paper presents an innovative access control model, referred to as Web service Access Control Version 1 (Ws-AC1), specifically tailored to Web services. The most distinguishing features of this model are the flexible granularity in protection objects and negotiation capabilities. Under Ws-AC1, an authorization can be associated with a single service and can specify for which parameter values the service can be authorized for use, thus providing a fine access control granularity. Ws-AC1 also supports coarse granularities in protection objects in that it provides the notion of service class under which several services can be grouped. Authorizations can then be associated with a service class and automatically propagated to each element in the class. The negotiation capabilities of Ws-AC1 are related to the negotiation of identity attributes and the service parameters. Identity attributes refer to information that a party requesting a service may need to submit in order to obtain the service. The access control policy model of Ws-AC1 supports the specification of policies in which conditions are stated, specifying the identity attributes to be provided and constraints on their values. In addition, conditions may also be specified against context parameters, such as time. To enhance privacy and security, the actual submission of these identity attributes is executed through a negotiation process. Parameters may also be negotiated when a subject requires use of a service with certain parameters values that, however, are not authorized under the policies in place. In this paper, we provide the formal definitions underlying our model and the relevant algorithms, such as the access control algorithm. We also present an encoding of our model in the Web Services Description Language (WSDL) standard for which we develop an extension, required to support Ws-AC1.

Keywords: access control; authorization; security; trust negotiation; WSDL

INTRODUCTION

Web services are a key component of the emerging, loosely coupled, Web-based computing architectural paradigm. They represent the core element for building complex application services provided either by single companies or by a set of cooperating companies. The area of Web services today, thus, is an active area characterized by academic research, industrial developments as well as standardization efforts.
However, despite such intense research and development efforts, current Web service technology does not provide yet the flexibility needed to “tailor” a Web service according to preferences of the requesting subjects, thus failing to fulfil the mass-customization promises made at the beginning of the Web services era. At the same time, Web service providers demand enhanced adaptivity capabilities in order to adapt the provisioning of a Web service to dynamic changes of the Web service “environment” according to their own policies. Altogether, these two requirements call for policy-driven access controls model and mechanisms, extended with negotiation capabilities.

Models and languages to specify access and management control policies have been widely investigated in the area of distributed systems (Damianou, Dulay, Lupu, & Sloman, 2001). Standardization bodies have also proposed policy-driven, standard access-control models (Oasis XACML, 2004). The main goals of such models are to separate the access control mechanism from the applications and to make the access control mechanism itself easily configurable according to different, easily deployable access control policies.

The characteristics of the open Web environment, where interacting subjects are mostly unknown to each other, has led to the development of the trust negotiation approach as a suitable access control model for this environment (Yu, Winslett, & Seamons, 2003; Herzberg, Mihaeli, Mass, Naor, & Ravid, 2000; Bertino, Ferrari, Squicciarini, 2003). Trust negotiation itself has been extended with adaptive access control, in order to adapt the system to dynamically changing security conditions (Ryutov, Zhou, Neuman, Leithead, & Seamons, 2005). In such work, a framework is proposed that integrates trust negotiation techniques with a middleware (Ryutov & Neuman, 2002), providing access control and application-level intrusion detection and response. Automated negotiation is also being actively investigated in different application domains, such as e-business and Grid computing. However, a common key requirement that has been highlighted is the need of a flexible negotiation approach that enables the system to dynamically adapt to changing conditions. In addition, the integration of trust negotiation techniques with Semantic Web technologies, such as semantic annotations and rule-oriented access control policies, has been proposed (Gavriloae, Nejdl, Olmedilla, Seamons, & Winslett, 2004). In this approach, the resource under the control of the access control policy is an item on the Semantic Web, with its salient properties represented as RDF properties. RDF metadata, managed as facts in logic programming, are associated with a resource and are used to determine which policies are applicable to the resource.

When extending a Web service with negotiation capabilities, the invocation of a Web service has to be managed as the last step of a conversation between the client and the Web service itself. The rules for such a conversation are defined by the negotiation protocol. Such a negotiation protocol should be described and made publicly available in a similar way as a Web service operation is publicly described through WSDL (W3C WSDL, 2005) declarations. An eXtensible Markup Language (XML)-based, machine-processable negotiation protocol description allows an electronic agent to automatically generate the messages needed to interact with the Web service. Of course, the client and the Web service must be equipped with a negotiation engine that evaluates the incoming messages, makes decisions and generates the outgoing messages according to the agreed-upon protocol.

The models already proposed for peer-to-peer negotiations assume that both parties are equipped with the same negotiation engine that implements the mutually understood negotiation protocol. This assumption, however, might not be realistic and may prevent the wide adoption of negotiation-enhanced access control models and mechanisms.

In this paper, we address the outlined requirements by proposing a Web service access control model and an associated negotiation protocol. The proposed model, Ws-AC1, is
Service Flavors: Differentiating Service Offerings in a Services Marketplace
[www.igi-global.com/article/service-flavors-differentiating-service-offerings/40898?camid=4v1a](www.igi-global.com/article/service-flavors-differentiating-service-offerings/40898?camid=4v1a)