Chapter 2.6
An Adaptive Access Control Model for Web Services

Elisa Bertino
Purdue University, USA

Anna C. Squcciarini
Purdue University, USA

Lorenzo Martino
Purdue University, USA

Federica Paci
University of Milano, Italy

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 & Neumman, 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 (Gavriloaie, 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 chapter, we address the outlined requirements by proposing a Web service access control model and an associated negotiation protocol. The proposed model, Ws-AC1, is based on a declarative and highly expressive access control policy language. Such a language allows one to specify authorizations containing conditions and constraints not only against the Web service parameters but also against the identity attributes of the party requesting the service and context parameters that can be bound, for example, to a monitor of the Web service operating environment. An additional distinguishing feature of Ws-AC1 is the range of object protection granularity it supports. Under Ws-AC1, the Web service security administrator can specify several access control policies for the same service, each one characterized by different constraints for the service parameters, or can specify a single policy that applies to all services in a set; to support such granularity, we