Chapter VI

Rafae Bhatti
IBM Almaden Research Center, USA

Daniel Sanz
Carlos III University of Madrid, Spain

Elisa Bertino
Purdue University, USA

Arif Ghafoor
Purdue University, USA

ABSTRACT

This chapter describes a policy-based authorization framework to apply fine-grained access control on Web services. The framework is designed as a profile of the well-known WS-policy specification tailored to meet the access control requirements in Web services by integrating WS-policy with an access control policy specification language, X-GTRBAC. The profile is aimed at bridging the gap between available policy standards for Web services and existing policy specification languages for access control. The profile supports the WS-Policy Attachment specification, which allows separate policies to be associated with multiple components of a Web service description, and one of our key contributions is an algorithm to compute the effective policy for the Web service given the multiple policy attachments. To allow Web service applications to use our solution, we have adopted a component-based design approach based on well-known UML notations. We have also prototyped our architecture in a loosely coupled Web services environment.
INTRODUCTION

Access control in Web services is a neglected frontier that has not seen the development and adoption of many standards, as opposed to the number of current and emerging specifications for authentication aspects of Web services security (WS Security, 2002; WS Trust, 2004; SAML, 2004). Several methods of authentication for Web services (such as SAML, WS-Security) have been proposed, which only help in authenticating the users, but do not differentiate between users in terms of fine-grained access privileges. This results in an all-or-nothing access which is not flexible enough for modern day business processes using Web services to execute. In this chapter, we address this requirement and present a policy-based authorization framework to apply fine-grained access control on Web services.

At the very onset, we would like to motivate the problem addressed in this chapter with a typical Web services scenario, which is depicted in Figure 1. It illustrates a health information system Web application that uses multiple Web services to offer a variety of services to its clients. It offers a top level service called patient track service (PTService) which allows physicians to track all patients in the system based on the authorization of the physician. This service returns a list of patients and the location of their records. Subsequently, the physician can choose to view a specific patient record from a given location (USA and Spain in this example), for which the system will invoke the appropriate Patient Record Service (PRService). The authorization credentials of the requesting physician will again be required to obtain this new service. The level of access that the physician is allowed will depend on his or her authorization credentials, and several instances of this Web service with a different set of operations corresponding to various levels of authorization may be defined to accommodate this requirement.

In this example, one would like to specify and enforce rules such as “a physician can access records generated in his/her own hospital, unless he/she obtains an authorization credential to view the records generated in other hospitals,” “physicians can only write records related to their specialization area,” or “nurses can read records representing prescriptions for patients that are under their care, when the system load is not high.” The specific service instance to invoke can be predefined or dynamically discovered (using, for instance, UDDI), but in both cases Web services description language (WSDL) specification (WSDL, 2001) is required to initiate the interaction. Clearly then, the task of interaction between

Figure 1. A Web-service based application: Services are described using WSDL documents