Authorization Service for Web Services and its Application in a Health Care Domain

Sarath Indrakanti, Macquarie University, Australia
Vijay Varadharajan, Macquarie University, Australia
Michael Hitchens, Macquarie University, Australia

ABSTRACT

In this paper, we discuss the design issues for an authorization framework for Web Services. In particular, we describe the features required for an authorization policy language for Web Services. We briefly introduce the authorization service provided by Microsoft .NET MyServices and describe our extended authorization model that proposes extensions to the .NET MyServices authorization service to support a range of authorization policies required in commercial systems. We discuss the application of the extended authorization model to a health care system built using Web Services. We use the XML Access Control Language (XACL) in our implementation to demonstrate our extended authorization model. This also enables us to evaluate the range of authorization policies that XACL supports.

Keywords: access control; authorization; policy language; security; Web Services

INTRODUCTION

Security plays a vital role in the design and practical deployment of distributed applications, as greater availability and access to information, in turn, imply that systems are more prone to attacks. In a networked computing system, when one principal requests a service from another, the receiving principal needs to address at least two fundamental questions: Is the requesting principal the one it claims to be? Does the requesting principal have appropriate privileges for the requested service? These two questions relate to the issues of authentication and authorization. The authorization requirements in networked applications are much richer than authentication both in terms of the types of privileges required and the nature and degree of interactions. There also are other security concerns, such as auditing, secure communication (confidentiality and integrity), availability, and accountability. All of these security issues apply in general to the Web Services architecture.
In general, security for Web Services is a broad and complex area covering a range of technologies. At present, there are several efforts underway that are striving for the provision of security services, such as authentication between participating entities, confidentiality, and integrity of communications. A variety of existing technologies can contribute to this area, such as TLS/SSL (Rescorla, 2001) and IPSec (Kent & Atkinson, 1998). We also have security functionality based on XML Signature (Bartel et al., 2002) and XML Encryption (Imamura et al., 2002) standards. There also are natural extensions of these to integrate security features in technologies such as SOAP (Gudgin et al., 2003) and WSDL (Christensen et al., 2001). WS-Security (Atkinson et al., 2002) specification describes enhancements to SOAP messaging to provide message integrity, confidentiality, and authentication. There also is work on XKMS (Ash et al., 2004) defining interfaces to key management and trust services based on SOAP and WSDL. There is a draft proposal on Web Services security policy language (Della-Libera et al., 2002) that describes the capabilities and constraints of the security policies on intermediary Web Services and end points. Web Services trust draft specification (Anderson et al., 2005) considers secure interoperation of Web Services by outlining a framework of trust models. There also is some work on Web Services privacy issues (O’Keefe & Greenfield, 2003). However, while there is a large amount of work on general access control and more recently on distributed authorization (Herzberg et al., 2000; Jajodia et al., 1997; Varadharajan et al., 1998), research in the area of authorization for Web Services is still at an early stage (Kraft, 2002; Yagüe & Troya, 2002). There is not yet a specification or a standard for Web Services authorization. Currently, most Web-service-based applications, having gone through the authentication process, make authorization decisions using application-specific access control functions, which result in the practice of frequently reinventing the wheel. This motivates us to have a closer look at the issues involved in designing an authorization framework for Web Services.

### DESIGN CHOICES FOR AUTHORIZATION

In some sense, there is a lot of similarities in the design of authorization services and frameworks for distributed applications and Web Services. Perhaps one aspect that makes it somewhat different in the case of Web Services is the need to take into account multiple domains and jurisdictions in a federated structure as a default. Although this is true in the case of distributed systems, as well, in the past the approach has been one of developing the service on a per-domain basis and then extrapolating it to multiple domains.

In designing a distributed authorization service for Web Services, there are some fundamental design issues that we need to address. First, we need to consider the types of authorization information to be used in the decision-making process. These range from static and generic information (e.g., identities) to specific information (e.g., roles) to dynamic and specific information, which are dependent on system state. Then, we need to address the class of authorization policies that need to be supported in the Web Services architecture. These can range from identity-based to role-based to delegation to joint actions to dynamic separation of duty. Associated with the different types of information, there can be different places at which checks need to be performed by different authorities. This, in turn, will lead to what authorization information (e.g., privileges or credentials) can be pushed to the decision-making authority and what information needs to be pulled, or a combination of both. Related to these is the replication strategy and who updates and manages what information and policies. Different design choices to these questions lead to different authorization frameworks that, in turn, need to be positioned within the distributed Web Services architecture. A detailed discussion of these issues can be found in
Metadata-Based Information Management Framework for Grids
Modern Technologies in Web Services Research (pp. 147-166).
www.igi-global.com/chapter/metadata-based-information-management-framework/26917?camid=4v1a