Chapter 2.11 PolyOrBAC: An Access Control Model for Inter-Organizational Web Services

Yves Deswarte
Université de Toulouse, LAAS-CNRS, France

Anas Abou El Kalam
Université de Toulouse, IRIT, INPT-ENSEEIHT, France

ABSTRACT

With the emergence of Web Services-based collaborative systems, new issues arise, in particular those related to security. In this context, Web Service access control should be studied, specified and enforced. This work proposes a new access control framework for Inter-Organizational Web Services: "PolyOrBAC". On the one hand, the authors extend OrBAC (Organization-Based Access Control Model) to specify rules for intra- as well as inter-organization access control; on the other hand, they enforce these rules by applying access control mechanisms dedicated to Web Services. Furthermore, the authors propose a runtime model checker for the interactions between collaborating organizations, to verify their compliance with previously signed contracts. In this respect, not only their security framework handles secure local and remote accesses, but also deals with competition and mutual suspicion between organizations, controls the Web Service workflows and audits the different interactions. In particular, every deviation from the signed contracts triggers an alarm, the concerned parties are notified, and audits can be used as evidence for a judge to sanction the party responsible for the deviation.

DOI: 10.4018/978-1-60566-650-1.ch044

1. INTRODUCTION

Web Services (WS) are increasingly gaining acceptance as a framework for facilitating application-to-application interactions within and across enterprises. In fact, WS facilitate the interoperability by providing abstractions as well as technologies for exposing enterprise applications as services and make them accessible through standardized interfaces (XML (World Wide Web Consortium [W3C], 2004), WSDL (W3C, 2006b), SOAP (W3C,2003)).

However, while much progress has been made toward providing interoperability, there is still a lot to do at the security level. In particular, a well-founded security study should identify who has access to what, when and in which conditions. The Common Criteria define an "*organizational security policy*" as: *a set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment* (Common Criteria for Information Technology Security Evaluation, 2006a). Such an organizational security policy usually relies on an *access control policy* (Common Criteria for Information Technology Security Evaluation, 2006b). An access control model is often used to rigorously specify and reason on the access control policy (e.g., to verify its consistency). However, the model does not specify *how* the security policy is enforced. The enforcement is realized by technical security mechanisms, such as credentials, cryptographic transformations (e.g., signature, encryption), access control lists (ACL), firewall rules, etc.

Moreover, in the context of an *AAA* architecture, not only it is important to specify and enforce *Authentication* and *Authorization,* but it is also necessary to achieve an efficient *Accounting*. This is extremely important in the WS context, in particular to prove infractions and to clearly identify the responsibilities in case of dispute or abuses.

Our major aim in this chapter is to define a global framework (*access control model and mechanisms*) for secure WS. In our study, we give a major attention and we progressively try to satisfy the following requirements:

- **Secure cooperation** between different organizations / users offering or using WS, but possibly mutually suspicious, with different services, features, functioning rules and security policies.
- **Loosely coupled organizations:** Each organization controls (and is responsible for) its own security policy, resources, applications, etc.
- **Decentralized** enforcement and administration of the security policies: each organization should enforce its own security policy with its own mechanisms.
- **Heterogeneity and self-determination:** As each organization is free to have its own WS, structure, OS, and local objects, it is the matter with heterogeneous systems where organizations keep some local self-determination. Actually, implementation details as well as private information should be managed by each organization, while remote accesses should be carried out through WS interfaces.
- **Fine-grained access control:** Access control decisions should take the context (e.g., specific situations, time and location constraints) into account. Moreover, as the context may change often and as certain reactivity is required in WS, organizations should support dynamic access rights.
- **Enforcement of permissions, explicit prohibitions as well as obligations.** In fact, explicit prohibitions can be particularly useful as we can have composite WS with decentralized policies where each administrator does not have details about the other parts of the system. Moreover, explicit prohibitions can also specify exceptions or limits the propagation of permissions in case of hierarchies. Similarly, obligations can be useful to impose some internal / external, manual / automatic actions that should be carried out by users