Chapter VII
Description of Policies Enriched by Semantics for Security Management

Félix J. García Clemente
University of Murcia, Spain

Gregorio Martínez Pérez
University of Murcia, Spain

Juan A. Botía Blaya
University of Murcia, Spain

Antonio F. Gómez Skarmeta
University of Murcia, Spain

ABSTRACT

Policies, which usually govern the behavior of networking services (e.g., security, QoS, mobility, etc.) are becoming an increasingly popular approach for the dynamic regulation of Web information systems. By appropriately managing policies, a system can be continuously adjusted to accommodate variations in externally imposed constraints and environmental conditions. The adoption of a policy-based approach for controlling a system requires an appropriate policy representation regarding both syntax and semantics, and the design and development of a policy management framework. In the context of the Web, the use of languages enriched with semantics has been limited primarily to represent Web content and services. However the capabilities of these languages, coupled with the availability of tools to manipulate them, make them well suited for many other kinds of applications, as policy representation and management. In this chapter, we present an evaluation of the ongoing efforts to use ontological (Semantic Web) languages to represent policies for distributed systems.
INTRODUCTION

The heterogeneity and complexity of computer systems is increasing constantly, but their management techniques are not changing and so system configuration processes are getting more complicated and error-prone. Therefore, there is a clear need for standardized mechanisms to manage advanced services and applications. Policy-based management (PBM) frameworks (Verma, 2000; Kosiur, 2001; Strassner, 2003) define languages, mechanisms and tools through which computer systems can be managed dynamically and homogeneously.

One of the main goals of policy-based management is to enable service and application control and management on a high abstraction level. The administrator specifies rules that describe domain-wide policies independent of the implementation of the particular service and/or application. It is then the policy management architecture that provides support to transform and distribute the policies to each node and thus to enforce a consistent configuration in all involved elements, which is a prerequisite for achieving end-to-end security services, or consistent access control configuration in different Web servers, for example.

The scope of policy-based management is increasingly going beyond its traditional applications in significant ways. The main functions of policy management architectures are:

- **Enforcement**: to implement a desired policy state through a set of management commands.

- **Monitoring**: ongoing active or passive examination of the information system, its services and applications for checking its status and whether policies are being satisfied or not.

- **Decision-taking**: to compare the current state of the communication system to a desired state described by a policy (or a set of them) and to decide how the desired state can be achieved or maintained.

In the information systems security field, a policy (i.e., security policy) can be defined as a set of rules and practices describing how an organization manages, protects, and distributes sensitive information. The research community, the industry, and standardization bodies have proposed different secure policy specification languages (Martínez Pérez, 2005) that range from formal policy languages that can be processed and interpreted easily and directly by a computer, to rule-based policy notation using if-then rules to express the mandatory behavior of the target system, and to the representation of policies as entries in a table consisting of multiple attributes. There are also ongoing standardization efforts toward common policy information models and frameworks such as CIM (Common Information Model) from the DMTF (Distributed Management Task Force, 2005).

In the Web services world, standards for SOAP-based message security and XML-based languages for access control are now appearing, as it is the case of XACML (OASIS, 2004). However the immaturity of the current tools along with the limited scope and total absence of explicit semantics of new languages make them less than-ideal candidates for sophisticated Web-based services or applications.

Ontological languages like OWL (Connolly et al., 2003) and others can be used to incorporate semantic expressiveness into the management information specifications and some reasoning capabilities which definitely would help in handling the management tasks aforementioned (i.e., enforcement, monitoring, and decision-taking). For example, in this kind of systems it is an important improvement to allow simple operations on different policies like testing equality, inclusion, equivalency and so. Ontological languages allow this kind of operations for the entities expressed with them.