IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com

ITB11705

This chapter appears in the book, *Web and Information Security*
edited by Elena Ferrari and Bhavani Thuraisingham © 2006, Idea Group Inc.

Chapter IX

Policy-Based Management of Web and Information Systems Security: An Emerging Technology

Gregorio Martínez Pérez, University of Murcia, Spain

Félix J. García Clemente, University of Murcia, Spain

Antonio F. Gómez Skarmeta, University of Murcia, Spain

Abstract

Network, service, and application management today faces numerous challenges, ones that older ways of doing things cannot solve. The concept of policy-based management (PBM) addresses some of these problems and offers possible solutions. It provides a system-wide view of the network and its services and applications, and shifts the emphasis of network management and monitoring away from specific devices and interfaces toward users and applications. This chapter describes the technology on the policy-based management paradigm which is considered

relevant for providing a common base for researchers and practitioners who need to understand the current status of this emerging technology and how it can be applied to the Web and information systems security field.

Introduction

One of the main goals of policy-based management (Kosiur, 2001; Strassner, 2003; Verma, 2000) is to enable network, service, and application control and management at a high abstraction layer. The administrator specifies rules that describe domain-wide policies which are independent of the implementation of the particular network node, 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 enforce a consistent configuration in all the elements involved. This is a prerequisite for achieving end-to-end security services or consistent access control configuration in different Web servers, for example.

The use of policies is an intrinsically layered approach allowing several levels of abstraction. There may be, for example, general policies expressing an abstract business goal, and on the other end, there may be policies that express a more specific device, service, or application dependent rule.

Policy rules are independent of a specific device and implementation, but they define a desired behavior in abstract terms. They are stored and interpreted by the policy framework, which provides a heterogeneous set of components and mechanisms that are able to represent, distribute, and manage policies in an unambiguous, interoperable manner, thus providing a consistent behavior in all affected policy enforcement points (i.e., entities where the policy decisions are actually enforced when the policy rule conditions evaluate to "true").

The main functions of policy management architectures are enforcement, that is, to implement a desired policy state through a set of management commands; monitoring, an ongoing active or passive examination of the network, its services, and applications for checking its status and whether policies are being satisfied; and decision making, that is, 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.