Chapter 4
Security Policy Specification

Jorge Bernal Bernabé
University of Murcia, Spain

Jesús D. Jiménez Re
University of Murcia, Spain

Juan M. Marín Pérez
University of Murcia, Spain

Félix J. García Clemente
University of Murcia, Spain

Jose M. Alcaraz Calero
Cloud and Security Lab Hewlett-Packard Laboratories, UK

Gregorio Martínez Pérez
University of Murcia, Spain

Antonio F. Gómez Skarmeta
University of Murcia, Spain

ABSTRACT

Policy-based management of information systems enables the specification of high-level policies which need to be refined into lower level configurations suitable to be directly applied to services and final devices in order to achieve the high-level behavior previous specified. This chapter presents a proposal for describing high-level security policies and for carrying out the policy refinement process for which low level policies and configurations are achieved. Firstly, an analysis of different research works related to the specification of security policy is provided. Then, a detailed description of the information model used for describing the information systems and the policies is described. After that, the language designed for specifying high level security policies is explained as well as the low level language based on the Common Information Model. Finally, some aspect about the policy refinement process done in the policy-based system in order to achieve low-level policies from the high-level security policies is outlined together with a description of the tools which can assist in the definition of the security policies and in the process refinement process.

INTRODUCTION

Information systems are incredibly growing nowadays becoming more and more complex to be administrated. Managing huge systems is a very complex problem and this issue has been focused in several research works during the last years proposing alternatives to tackle different aspects of system management. An approach is the management of systems based on policies. It enables the specification of high level business policies which are refined into low-level policies suitable to be directly applied into final devices to achieve the high-level behavior previous specified.

DOI: 10.4018/978-1-4666-1888-6.ch004

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Security is a key aspect to be controlled in information systems and policy-based systems can help to control it. To this end, security policies can be described by administrators using a language designed for this purpose which enables the description of high level security policies. Researchers have proposed multiple approaches for policy specification that range from formal policy languages that a computer can directly process and interpret, to rule-based policy notation using an if-then-else format. The definition and the usage of high level policy languages ease the process of policy specification reducing significantly errors therein. In fact, high-level policies require less effort to be written and maintained since a lot of details are hidden to writers. Note that this kind of policies does not need training or deep knowledge to be used even by (maybe not so skilled) administrators. This is especially suitable in security field in which any specification error potentially may cause a security hole in the information system.

In the policy definition process, the task of a policy manager is to transform the business policies into implementable policies using a formal language for this purpose. To do so, the manager uses a high level policy language that assures that the representation of security policies will be unambiguous and verifiable. Moreover, other important requirements of any policy language are:

- **Clear and well defined semantics:** The semantics of a policy language can be considered as well defined if the meaning of a policy written in this language is unambiguous at any time of its life-cycle.
- **Flexibility and extensibility:** A policy language has to be flexible enough to allow new policy information to be expressed, and extensible enough to allow new semantics to be added in future versions of this language.
- **Independent of the administrative domain:** where it will be used and, in particular, of manufacturers/providers of devices and services. A policy language is independent if a policy written in this language is independent of a specific deployment.
- **Readability:** A policy language must be easy to understand when read by the administrator.
- **Amenable to combining:** A policy language should include a way of grouping policies.

In addition, a policy language should facilitate the realization of functions related to policy framework. In this sense, other requirements are:

- **Access to policy information:** A policy representation oriented to facilitate queries about policy information.
- **Conflict detection:** A policy language which facilitates the process of conflict detection, either enabling a direct integration in conflict analysis tools, or having syntactic and semantics elements to facilitate the conflict analysis.
- **Policy distribution:** The policy representation may support of multiple bindings that is to be possible to convey policy instances in a number of different protocols.
- **Policy refinement:** A policy language may provide facilities or techniques to help in the policy translation process and to achieve policy and rules consistent at every level of abstraction.

This book chapter describes a proposal for describing high level security policies and for carrying out the policy refinement process for which low level policies are achieved, which can be directly applied over the final devices. First, an analysis of different research works related to the specification of security policy is provided in this chapter. Then, a detailed description of the information model used for describing the information systems and the policies is provided.

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/security-policy-specification/67499

Related Content

Game-Based Control Mechanisms for Cognitive Radio Networks
(2014). *Game Theory Applications in Network Design (pp. 352-400).*
www.irma-international.org/chapter/game-based-control-mechanisms-for-cognitive-radio-networks/109816

Internet of Things: Privacy and Security Implications
Mohamed A. Eltayeb (2017). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-18).*
www.irma-international.org/article/internet-of-things/179894

Power Control Schemes Based on Game Theory
(2014). *Game Theory Applications in Network Design (pp. 244-276).*
www.irma-international.org/chapter/power-control-schemes-based-on-game-theory/109813

Optical Transport Network: A Physical Layer Perspective Part 1
(2015). *Optical Transmission and Networks for Next Generation Internet Traffic Highways (pp. 1-27).*
www.irma-international.org/chapter/optical-transport-network/117809

Economic Crisis in Colombia Due to COVID-19: From Pandemic to Post-Pandemic Actions
Jahir Lombana-Coy, María Carolina Ovalleand Alberto Elías Muñoz Santiago (2022). *Handbook of Research on Global Networking Post COVID-19 (pp. 110-129).*
www.irma-international.org/chapter/economic-crisis-in-colombia-due-to-covid-19/309603