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

ITB11704

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

Chapter VIII

Integrating Access Policies into the Development Process of Hypermedia Web Systems

Paloma Díaz, Universidad Carlos III de Madrid, Spain

Daniel Sanz, Universidad Carlos III de Madrid, Spain

Susana Montero, Universidad Carlos III de Madrid, Spain

Ignacio Aedo, Universidad Carlos III de Madrid, Spain

Abstract

This chapter discusses the integration of access control in the development process of hypermedia applications. Two key ideas are proposed: the use of high level, abstract access control models and the inclusion of access control in the whole life cycle of hypermedia applications. Authors present an access control model for hypermedia that makes it possible to formalize access policies using elements of the hypermedia domain, those used to specify structure and navigation services. Abstract models are not enough

to assist developers in dealing with security in a systematic way. Thus, authors describe how high-level access rules can be specified following the Ariadne Development Method (ADM). The ARCE project is used as example of development.

Introduction

The hypermedia paradigm organizes information as an associative net of nodes that can be freely browsed by selecting links and using navigation tools such as indexes, breadcrumbs, or maps. From the point of view of the application, Web sites are a subclass of hypermedia systems that use a specific technology to manage and deploy information but share the same access philosophy, and, for that reason, we will use the term hypermedia Web system to denote a special case of hypermedia. Access control is an essential requirement in hypermedia Web systems. Most companies and organizations are taking profit from the distributed nature of the Web to provide advanced services to authorized users (e.g., financial transactions). During the development process of hypermedia Web systems, access requirements have to be tackled from different levels of abstraction (Fernández et al., 1996) and not just as implementation decisions. At the highest level of abstraction, the focus of this chapter, access models provide formal mechanisms to determine who can or cannot do what with which components of the hypermedia Web system, that is, to specify the access rules, both the positive as well as the negative, that establish a safe system operation. In fact, a security model for hypermedia/Web allows formalization of access policies using components and services that belong to the hypermedia domain, the same as those used for the specification of other system features (i.e., structure and navigation services). Thus, developers will be able to decide and discuss issues such as which hypermedia nodes can be accessed, which information items are to be delivered in each node, or which links are to be made available according to users' permissions, without being aware of how and where hypermedia components are physically stored. It is important to note that high-level models are not enough to assist developers in dealing with security in the systematic way that distinguishes engineering from other disciplines. Access modeling has to be integrated into the whole development process (Devanbu & Stubblebine, 2000), so that, from the beginning of the project, developers know how to specify access policies and how to relate