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
ITB11699

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

Chapter III

Policies for Web Security Services

Konstantina Stoupa, Aristotle University of Thessaloniki, Greece

Athena Vakali, Aristotle University of Thessaloniki, Greece

Abstract

This chapter analyzes the various types of policies implemented by the Web security services. According to X.800 definition, there are five basic Web security services categories: authentication, non-repudiation, access control, data integrity, and data confidentiality. In this chapter, we discuss access control and data privacy services. Access control services may adopt various models according to the needs of the protected environment. In order to guide the design of access control models, several policy-expressing languages have been standardized. Our contribution is to describe and compare the various models and languages. Data privacy policies are categorized according to their purpose, that is, whether they express promises and preferences, manage the dissemination of privacy preferences, or handle the fulfillment of the privacy promises.

The chapter is enriched with a discussion on the future trends in access control and data privacy.

Introduction

Today, users adopt the Internet to complete several business and commercial transactions. The introduction of Web services has enriched this trend. According to Cerami (2002), "a Web service is any service that is available over the Internet, uses a standardized XML messaging system, and is not tied to any one operating system or programming language." As a consequence to their wide adoption, Web services have become the core target of malicious attacks (aiming at either stealing information or causing services and system malfunctions). Therefore, Web-accessed environments need to employ security services to protect their resources (either information or services). Such services enhance the security of data processing, information transferring, and organizational data circulation. Security and protection of Web databases and services have become core research issues, and recent research efforts have focused on these topics (Ferrari & Thuraisingham, 2004; Ferrari, 2004; Thuraisingham, 2002). Overall, security services ensure both secure communication and storage of data, and the proper and continuous execution of Web services.

According to X.800 definition, five basic security services categories exist: *authentication, access control, data confidentiality, data integrity,* and *non-repudiation.* Each of these security services employs security policies which are implemented by security mechanisms (e.g., RFC 2828 glossary). More specifically, we categorize services into:

- **Services for clients' and resources' identities:** verifying the identity of the requesting client and preventing client attempts to deny having accessed a protected resource. Thus, this category involves :
  - **Authentication services:** to verify an identity claimed by (or for) an entity.
  - **Non-repudiation services:** to prevent either sender or receiver from denying a transmitted message.