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

ITB11698

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

Chapter II

Web Services Security

Carlos A. Gutiérrez García,
Sistemas Técnicos de Loterías del Estado, Spain

Eduardo Fernández-Medina Patón,
Universidad de Castilla-La Mancha, Spain

Mario Piattini Velthius,
Universidad de Castilla-La Mancha, Spain

Abstract

During the past few years, significant standardization work in the Web services (WS) technology area has been performed. As a consequence of these initial efforts, WS foundational stable specifications have already been delivered. Now, it is time for the industry to standardize and address the security issues that have emerged from this paradigm. Up until now, much activity has been carried out on this subject. In this chapter, we will specify the main security services that have to be addressed in the WS world as well as a description of the aspects already addressed and unaddressed. We will mention the main initiatives and their respective specifications that try to cover the distinct security issues within the WS outlook. Whenever possible, unaddressed security issues for each topic will be stated. In addition, current general security concerns will be detailed, and future research will be proposed.

Background

During the past few years, the Web services (WS) paradigm has achieved great popularity and is currently a new buzzword among middleware and enterprise software specialists. Technologies derived from this paradigm have reached such a maturity level that now they can be considered as the most promising full-fledged and standard integration solutions. Hence, WS has become a reality on which IT departments are basing their operations to achieve a direct alignment with the business operations they support (Casati, Shan, Dayal, & Shan, 2003). In fact, according to the most recent reports from IDC, over the next years, the market for WS solutions will grow steadily reaching $11 billion in 2008 (IDC, 2004).

Perhaps the most precise and practical definition of the term *WS* is provided by the W3C Web Services Architecture Working Group: "A Web service is a software application identified by a URI, whose interfaces and bindings are capable of being defined, described, and discovered as XML artifacts. A Web service supports direct interactions with other software agents using XML-based messages exchanged via Internet-based protocols" (W3C, 2004).

WS are distributed, decentralized, self-contained, self-describing; can be dynamically published, located, invoked; are language independent and interoperable, inherently open, standards based; and are able to be composed and provide well-defined services to certain service consumers (Endrei et al., 2004). Consequently, WS based-solutions must be concerned with typical security problems that are common to distributed communications, through a compromised channel, between two or more parties. Some of the major inherited security issues that WS technologies must address are authentication, authorization, confidentiality, data integrity, non-repudiation, and availability (Sedukhin, 2003). WS must address both the issues inherited from the distributed computing classical scheme and those arising from the new threats created by its own nature.

In addition, ways to protect service providers and service consumers are needed. For example, service providers can be protected by applying control access mechanisms to the services (OASIS, 2003b) or information (Shandu, Coyne, Feinstein, & Youman, 1996) they own or by guaranteeing non-repudiation of the interactions they perform. On the other hand, service consumers' protection is mainly focused on service trustworthiness and data privacy concerns. Service trustworthiness assures service consumers that the

Related Content