Chapter II

Privacy Issues in the Web Services Architecture (WSA)

Barbara Carminati, University of Insubria at Como, Italy

Elena Ferrari, University of Insubria at Como, Italy

Patrick C. K. Hung, University of Ontario Institute of Technology (UOIT), Canada

Abstract

A Web service is a software system that supports interoperable application-to-application interactions over a network. Web services are based on a set of XML standards such as Universal Description, Discovery and Integration (UDDI), Web Services Description Language (WSDL), and Simple Object Access Protocol (SOAP). Recently, there have been increasing demands and discussions about Web services privacy technologies in the industry and research community. To enable privacy protection for Web service consumers across multiple domains and services, the World Wide Web Consortium (W3C) published a document called "Web Services Architecture (WSA) Requirements" that defines some fundamental privacy requirements for Web services. However, no comprehensive solutions to the various privacy issues have been so far defined. For these reasons, this chapter will focus on privacy technologies by first discussing the main privacy issues in WSA and related protocols. Then, this chapter illustrates the standardization efforts going on in the context of privacy for Web services and proposes different technical approaches to tackle the privacy issues.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Introduction

Privacy is a state or condition of limited access to a person (Schoeman, 1984). Information privacy relates to an individual’s right to determine how, when, and to what extent information about the self will be released to another person or to an organization (Leino-Kilpi, Dassen, Gasull, Lemonidou, Scott, & Arndt, 2001). Threats to information privacy can come from insiders and from outsiders in each organization (Fischer-Hubner, 2001). In general, privacy policies describe what information an organization collects from individuals (e.g., consumers) and what (e.g., purposes) they do with it. Many studies show that good privacy protection is an important factor to generate a good business (Bennett, 1997).

In the U.S., the Privacy Act of 1974 (Fischer-Hubner, 2001) requires that federal agencies grant individuals access to their identifiable records that are maintained by the agency, ensure that existing information is accurate and timely, and limit the collection of unnecessary information and the disclosure of identifiable information to third parties. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs privacy issues related to collected data, including those collected via traditional Web-based applications (PIPEDA, 2005). On the reverse, the Europe Union Data Protection Directive (Steinke, 2002) contains two statements contradicting the U.S. one. The first statement requires that an organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization, and the types of third parties to which it discloses the information. The second statement requires that personal data on EU citizens may only be transferred to countries outside the 15 nation block that adopt these rules or are deemed to provide “adequate protection” for the data. As a result, these statements imply that no information of any EU citizen can be transferred to the U.S. due to the conflicts between two privacy acts. Consequently this creates obstacles for conducting business activities between these two regions. To overcome the difficulties, the U.S. government already has a voluntary scheme called “Safe Harbour” to provide an adequate level of data protection which can safeguard transfers of personal data to the U.S. from EU. The U.S. companies doing business in the EU must certify to the Commerce Department that they will follow the regulations of the EU directive. Any violation would be subject to prosecution by the Federal Trade Commission (FTC) for deceptive business practices.

For instance, biometrics (Grijpink, 2001) and healthcare applications (Cheng & Hung, 2005) have to seriously enforce privacy protection. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rules (HL7, 2004) in the U.S., Protected Health Information (PHI) includes individually identifiable health information related to past, present, and future physical and mental health conditions, as well as the past, present, and future payment for the provisions of healthcare to an individual. HIPAA provided a set of standard policies that the healthcare providers must exercise in order to protect a patient’s privacy. HIPAA provides a standard set of electronic transaction formats and regulations to ensure the privacy and security of healthcare-related transactions. Similarly, the Personal Health Information Protection Act of 2004 (PHIPA) in Canada establishes rules for the collection, use, and disclosure of personal health information about individuals that protect the confidentiality of that information.