Chapter 15
Security for Web Services:
Standards and Research Issues

Lorenzo D. Martino
Purdue University, USA

Elisa Bertino
Purdue University, USA

ABSTRACT
This article discusses the main security requirements for Web services and it describes how such security requirements are addressed by standards for Web services security recently developed or under development by various standardizations bodies. Standards are reviewed according to a conceptual framework that groups them by the main functionalities they provide. Covered standards include most of the standards encompassed by the original Web Service Security roadmap proposed by Microsoft and IBM in 2002 (Microsoft and IBM 2002). They range from the ones geared toward message and conversation security and reliability to those developed for providing interoperable Single Sign On and Identity Management functions in federated organizations. The latter include Security Assertion Markup Language (SAML), WS-Policy, XACML, that is related to access control and has been recently extended with a profile for Web services access control; XKMS and WS-Trust; WS-Federation, LibertyAlliance and Shibboleth, that address the important problem of identity management in federated organizations. The article also discusses the issues related to the use of the standards and open research issues in the area of access control for Web services and innovative digital identity management techniques are outlined.

DOI: 10.4018/978-1-61350-104-7.ch015
INTRODUCTION

Today Web services are a fundamental component of agile e-business. Through the use of eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP) (Gudgin, 2007), and related open standards deployed in Service Oriented Architectures (SOA), they allow data and applications to interact through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can co-exist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases. Interoperability is a key requirement for Web services and, at the same time, it is the key objective and promise of the standardization effort. Web services enhance interoperability and are thus able to support business applications composed by chains of Web services. Interoperability is a key promise of Web service technology and therefore notions such as Web service composition and technologies like workflow systems are being investigated and developed.

The use of Web services, stand-alone or composed, must however provide strong security guarantees. Security is today a relevant requirement for any distributed application, and in particular for those enabled by the Web such as e-health, e-commerce, e-learning. Providing security guarantees in open dynamic environments characterized by heterogeneous platforms is however a major challenge. Web services security encompasses several requirements that can be described along the well known security dimensions:

- Integrity, whereby information can be modified only by users who have the right to do so, and only in authorized ways. In particular, message integrity requires that a message remain unaltered during transmission. Ensuring information integrity might also require that information is transferred only among intended users and in intended ways.
- Confidentiality, whereby information can be disclosed only to users authorized to access it. When applied to messages, it requires that the content of a message cannot be viewed while in transit, except by authorized services.
- Availability, whereby the use of the system cannot be denied to entitled users inadvertently or due to denial of service attacks by a malicious party.
- Accountability, whereby users are accountable for their security-relevant actions. A particular case of this is non-repudiation, where responsibility for an action cannot be denied.

Furthermore, each Web service must protect its own resources against unauthorized access. This in turn requires suitable means for: identification, whereby the recipient of a message must be able to identify the sender; authentication, whereby the recipient of a message needs to verify the claimed identity of the sender; authorization, whereby the recipient of a message applies access control policies to determine whether the sender has the right to use the required Web service and other protected resources. In a Web service environment it is however not enough to protect the service providers, it is also important to protect the parties requiring services. Since a key component of the Web service architectures is represented by the discovery of services, it is crucial to ensure that all information used by parties to this purpose be authentic and correct. Also we need approaches by which a service provider can prove its identity to the party requiring the service in order to avoid attacks, such as phishing attacks.

Within this context, the goal of securing Web services can be decomposed in three broad subsidiary goals: