Category: Concepts, Trends, and Challenges

Web Services' Security

Fergle D'Aubeterre
The University of North Carolina at Greensboro, USA

A. F. Salam
The University of North Carolina at Greensboro, USA

INTRODUCTION

Web services provide a standard architecture for heterogeneous systems to share and exchange information over the Internet (Iyer, Freedman, Gaynor, & Wyner, 2003). In this context, Web services are based on the building-block approach of using prior Internet protocols and standards as components of Web services. The building blocks include HTTP, adopted as the transport protocol, and XML, used as the format of the messages that are transferred between cooperating applications (Lim & Wen, 2003).

For e-businesses to fully realize the benefits of Web services, security issues need to be addressed. Security has become a major concern for all enterprises exposing sensitive data and business processes as Web services (Bhatti, Bertino, Ghafoor, & Joshi, 2004). In this regard, this research proposes an integrated security approach for Web services architecture.

The proposed approach, which is an addendum to the Web services security specifications, is built on XML-role-based access control (RBAC) for Web services business processes. Basically, it supports protocol-independent declarative security policies that can be enforced by Web service providers, and descriptive security policies that clients can use to access the services in a secure manner.

BACKGROUND

The sharing of information and knowledge resources is the main motivation for constructing distributed systems. According to Coulouris et al. (2001), a distributed system is one in which components located at network computers communicate their actions only by passing messages. Today, e-commerce is evolving into a dynamic business network where participants have distinct IT platforms and applications. The problems associated with heterogeneity in platforms and applications require technological solution that provides integration without sacrificing past IT investments. In this context, Web services can be considered as the best choice from the different options among distributed environments (Iyer et al., 2003).

Before entering into the security aspects of Web services, it is of vital importance to understand what Web services are. Sleeper (2001, p. 1) defined Web services as "loosely coupled, reusable software components that semantically encapsulate discrete functionality and are distributed and programmatically accessible over standard Internet protocols." In other words, Web services provide a standard way for heterogeneous applications to share and exchange information. Web services are based on the following open standards (Iyer et al., 2003):

- Simple object access protocol (SOAP),
- Extensible markup language (XML),
- Web services description language (WSDL),
- Application programming interface (API), and
- Universal description, discovery, and integration (UDDI) (See Key Terms for more information).

Web service is conceived as a new paradigm for distributed computing environments. However, Web services architecture is still vulnerable to potential security threats (Chatterjee & Webber, 2004). For instance, some of the message level security threats include: message alteration, confidentiality, man-in-the-middle, snooping, denial of service (DoS), and reply attacks.

The most common security techniques used for overcoming these issues are the following: authentication mechanisms, authorization, data integrity and data confidentiality, integrity of transactions and communications, non-repudiation, end-to-end integrity and confidentiality of message, audit trial, and distributed enforcement of security policies. However, such techniques by themselves are not sufficient because they do not consider the holistic view of the e-business processes' security.

The foundation of Web services security is the Web services security plan and roadmap developed by IBM and Microsoft (IBM & Microsoft, 2002). The specifications of this security roadmap are WS-Security, WS-Policy, WS-Trust, WS-Privacy, WS-SecureConversation, WS-Federation, and WS-Authorization.

Several models to address Web-Services security issues have been proposed. In this regard, Joshi et al. (2001) provided an evaluation and comparison of the discretionary access control (DAC) model, the mandatory access control (MAC) model, and the role-based access control (RBAC) model.

The RBAC models have received wide acceptance. They classify the elements of the system into users, roles, permissions, operations, and objects. Because the administration of RBAC is separated from its access control functions, the security administration is made easier and more efficient (Bhatti et al., 2004; Sandhu, Coyne, &Youman, 1996). In addition, a very important characteristic of RBAC models is that they are able to represent organization policies. Chen and Sandhu (1996), who established the foundations for constraints RBAC, explained how organizations policies can be represented and enforced using constraints. In the context of Web services, RBAC does not incorporate the content and context of the information workflow; therefore, RBAC is not appropriate to secure Web services transactions.

Koshutanshi and Massacci (2003) proposed a security architecture for orchestrating authorization and security of the Web services processes (see Figure 1).

The XML-based RBAC approach proposed by Bhatti et al. (2004) provides access control for Web services at the element-level granularity. This approach includes the core RBAC primary elements (users, roles, permissions, operations, and object) as well as the role hierarchies and separation of duty constraints (Bhatti, Joshi, Bertino, & Ghafoor, 2003; Ferraiolo, Sandhu, Gavrila, Kuhn, & Chandramouli, 2001). Moreover, in order to capture the context information, this approach utilizes a location-based technique. Bhatti et al. (2004) uses XML-based specification language to represent each RBAC element and their relationships.

As it was mentioned earlier, Web services still present security issues that need to be addressed. According to Joshi et al. (2001), in order to take care of the Web-based security issues, comprehensive security frameworks are required. Hondo et al. (2002) stated that a Web service security model must support protocol-independent declarative security policies that Web service providers can enforce, and descriptive security policies attached to the service definitions that clients can use in order to securely access the service.

Even though Koshutanshi and Massacci (2003) approach addresses many security issues related to Web Services processes and information flows, it is still not sufficient. The framework by itself secures only the Web services processes and information flows from the client, which can be seen as an enterprise to the application server and vice-versa. As a result, the security of the Web services processes and information flows within the client (enterprise) is neglected. However, using the access control model created by Bhatti et al. (2004), the Web services process and information flows within the enterprise can be secured.

Using Bhatti et al. (2004) and Koshutanki and Masacci (2003) models as a foundation, an integrated architecture for Web services security is developed. Such architecture allows Web services business processes and information flows to be secured across enterprises, and at the same time inside of each enterprise.

A NEW APPROACH FOR EXTENDING THE WEB SERVICES' SECURITY

Essentially, the proposed approach provides for controlled access, secure sharing and distribution of information based on content and context, secure workflows, and secure interoperation in a Web services environment. It is important to keep in mind, that the proposed approach is an addendum to the Web services security specifications. Moreover, it is assumed that for securing the message the W3C and the IETF specification for the XML-signature (Bartel, Boyer, Fox, MaMacchia, & Simon, 2002) and W3C XML-encryption (Imamura, Dillway, & Simon, 2002) are being used. Figure 2 shows the proposed architecture.

The proposed architecture for Web services security consists of different components that interact in two different stages: client registration and client authorization. Figure 3 presents the building blocks of the pro-

Figure 1. Cross-section view of the architecture (Koshutanshi & Massacci, 2003)