Chapter 41
Developing Proactive Security Dimensions for SOA

Hany F. EL Yamany
Suez Canal University, Egypt

David S. Allison
The University of Western Ontario, Canada

Miriam A. M. Capretz
The University of Western Ontario, Canada

ABSTRACT

Security is one of the largest challenges facing the development of a Service-Oriented Architecture (SOA). This is due to the fact that SOA security is the responsibility of both the service consumer and service provider. In recent years, many solutions have been implemented, such as the Web Services Security Standards, including WS-Security and WS-SecurityPolicy. However, those standards are insufficient for the promising new generations of Web 2.0 applications. In this research, we describe an Intelligent SOA Security (ISOAS) framework and introduce four of its services: Authentication and Security Service (NSS), the Authorization Service (AS), the Privacy Service (PS) and the Service of Quality of Security Service (SQoSS). Furthermore, a case study is presented to examine the behavior of the described security services inside a market SOA environment.

INTRODUCTION

Service-Oriented Architecture (SOA) is a software architecture that is based on the key concepts of an application front end, a service, a service repository, and a service bus. SOA includes three main components: the service provider, who offers a service, the service consumer, who seeks to access the provider's service, and the service repository, where the provider can publish his/her services for discovery by the consumer (Erl, 2005).

One of the major challenges in designing SOA involves developing its security requirements. SOA security is an overarching concern, as it affects every advertisement, discovery and interaction of services and applications in an SOA environment. Specifically, SOA security generally requires authentication, privacy, auditing and

DOI: 10.4018/978-1-4666-2919-6.ch041

authorization. Authentication entails the validation of identity, while privacy guarantees the nondisclosure of an individual's data. Moreover, auditing makes a user accountable for the messages that they send, while authorization establishes the actions that a user is allowed to perform (Erl, 2005). SOA security is the responsibility of both the service provider and consumer, since they share much of the same resources and data. Organizing SOA security is an intensive endeavor, which involves coordinating different security requirements for the service provider and consumer.

Another challenge of SOA security requirements involves an increase in flexibility for incorporating Quality of Service (QoS) terms, such as reliability and security, which fulfill the various requirements of customers. QoS requirements entail a commitment to a certain level of service, which is based on a measurable set of parameters. According to these parameters, the level of service can indicate the amount of security in terms of variables such as assurance and mechanical strength.

This chapter aims to describe and design an intelligent framework for SOA security. The suggested SOA security framework includes five services that incorporate the most important security aspects: authentication, authorization, Quality of Security Service, privacy, and auditing. Each service encapsulates its own security logic, which can be consequently published, discovered, and reused. Moreover, almost all of the services embed an intelligent core in order to automate the security processes.

The chapter begins with an investigation into related work in the field of SOA security. Following this review, four of the described services are discussed in detail, through an introduction of their objectives, structures, intelligent core and implementation; these services include the Authentication and Security Service (NSS), the Authorization Service (AS), the Privacy Service (PS) and the Service of Quality of Security Service (SQoSS). The Intelligent SOA Security (ISOAS) framework is shown in Figure 1.

At the end of this chapter, a case study is introduced to establish the interactions among the services within the SOA security framework in order to provide the sufficient and necessary security dimensions for an SOA environment.

BACKGROUND

Researchers in educational institutions as well as in companies such as Microsoft, Oracle and IBM, are devoting time and effort to developing and maintaining security solutions for SOA. One of the most remarkable industrial studies has been introduced by IBM, who has announced its proposal for a complete security model of SOA applications, especially those within banking systems (Buecker et al., 2007). The suggested IBM model consists of three basic levels: Business Security Services, Security Policy Infrastructure and IT Security Service. Overall, the framework discusses most of the security issues involved in an SOA environment, and it is primarily designed based on the Web Services Standards.

Both similarities and differences exist between the IBM SOA security model (Buecker et al., 2007) and the ISOAS framework discussed in this chapter. In terms of similarities, both frameworks manage most of the SOA security aspects, including authentication and authorization. Also, both frameworks follow the SOA security approaches, such as Security as a Service, for managing the SOA security aspects and the required security levels, including the Message and Services Levels. Finally, the authentication service in each framework can utilize several security tokens in order to authenticate the different service consumers.

On the other hand, there are several differences between the two frameworks; for example, the ISOAS framework contains many intelligent engines in order to automatically manage the security