Chapter 1.39
Security in Service-Oriented Architecture:
Issues, Standards, and Implementations

Srinivas Padmanabhuni
Software Engineering and Technology Labs, Infosys Technology Limited, India

Hemant Adarkar
Ness Technologies, India

ABSTRACT

This chapter covers the different facets of security as applicable to Service-Oriented Architecture (SOA) implementations. First, it examines the security requirements in SOA implementations, highlighting the differences as compared to the requirements of generic online systems. Later, it discusses the different solution mechanisms to address these requirements in SOA implementations. In the context of Web services, the predominant SOA implementation standards have a crucial role to play. This chapter critically examines the crucial Web services security standards in different stages of adoption and standardization. Later, this chapter examines the present-day common nonstandard security mechanisms of SOA implementations. Towards the end, it discusses the future trends in security for SOA implementations with special bearing on the role of standards. The authors believe that the pragmatic analysis of the multiple facets of security in SOA implementations provided here will serve as a guide for SOA security practitioners.

INTRODUCTION

Security is a fundamental issue of concern in computing systems. With the recent trends in distributed computing, primarily the emergence of World Wide Web (WWW) as a universal medium for conducting business, security has become critical in IT architectures. Successful Web security mechanisms like Secure Sockets Layer (SSL) have played a critical role in the emergence of WWW as a mainstream technology with wide acceptance.

In the context of distributed systems, SOA has caught the critical attention of both technology and business champions alike because of its

promise in removing some of the hurdles in earlier models of distributed computing. Though SOA as a concept is not new, this promise is based on the open and loosely coupled nature of the newer SOA implementations.

In this chapter, we are concerned with multiple dimensions of security in loosely coupled SOA implementations. Web services, the most prevalent SOA implementation, represent an extension of the paradigm of Web. Web services represent applications that can be invoked over open networks using standard Web-based protocols. Other upcoming SOA implementations include Jini (Jini Spec, 2003), Open Grid Services Architecture (OGSA) (OGSA Spec, 2003), and so forth. We shall cover the various security requirements in SOA implementations, highlighting the differences from security requirements in generic online systems. We shall proceed to cover the different solution mechanisms to address these requirements in SOA implementations. Later, we shall explore the Web services security standards in detail. We shall then proceed to explore the common nonstandard security mechanisms of today, addressing Web services security. Towards the end, we shall present the future trends in security for SOA implementations including Web services.

BACKGROUND

Since we are concerned with security of loosely coupled SOA implementations, we shall cover the generic security requirements and solutions in online systems, alongside the core concepts in SOA.

While online systems have been in use for the past few decades, the advent of the Web as a commercial medium has posed significant security challenges due to its public and open nature. Further, e-business and e-commerce has placed stringent security requirements due to the online transactions involved. Current security technologies in Web are able to handle and manage the expectations for e-commerce and e-business transactions. Security, in effect, broadly reflects a collection of security requirements to be satisfied. In this section, we point out the primary security requirements in online systems. Some of the typical security requirements of online systems are outlined below:

- **Confidentiality:** The confidentiality requirement states that any piece of information should not be understood by anyone other than the person for whom it was intended. Message privacy is a key requirement here.
- **Data Integrity:** The integrity requirement states that information should not be altered in storage or transit between a sender and the intended receiver without the alteration being detected.
- **Authentication:** The authentication requirement states that the sender and receiver should be able to confirm each other's identity and the origin/destination of the information.
- **Authorization:** The authorization requirement ensures that the sender has the required authority to perform the operation. This may range from permission to perform some action to permission for viewing some content.
- **Non-repudiation:** The nonrepudiation requirement ensures that the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- **Privacy:** The privacy requirement is more general than the confidentiality requirement above. It also deals with the question of whether to trust the personal information with a Web site.
- **Trust:** This refers to the confidence in a person or a partner doing the transaction. This concept extends beyond trust in a person accessing an online service to even