Chapter 12
Model–Driven Approach for End–to–End SOA Security Configurations

Fumiko Satoh
IBM Research – Tokyo, Japan

Yuichi Nakamura
IBM Research – Tokyo, Japan

Nirmal K. Mukhi
IBM Research – Thomas J. Watson Research Center, USA

Michiaki Tatsubori
IBM Research – Tokyo, Japan

Kouichi Ono
IBM Research – Tokyo, Japan

ABSTRACT

The configuration of non-functional requirements, such as security, has become important for SOA applications, but the configuration process has not been discussed comprehensively. In current development processes, the security requirements are not considered in upstream phases and a developer at a downstream phase is responsible for writing the security configuration. However, configuring security requirements properly is quite difficult for developers because the SOA security is cross-domain and all required information is not available in the downstream phase. To resolve this problem, this chapter clarifies how to configure security in the SOA application development process and defines the developer’s roles in each phase. Additionally, it proposes a supporting technology to generate security configurations: Model-Driven Security. The authors propose a methodology for end-to-end security configuration for SOA applications and tools for generating detailed security configurations from the requirements specified in upstream phases model transformations, making it possible to configure security properly without increasing developers’ workloads.

DOI: 10.4018/978-1-60566-794-2.ch012
INTRODUCTION

Service-Oriented Architecture (SOA) is an important concept that is useful for building applications for enterprise business processes, because an application based on SOA can change its business processes flexibly. Unfortunately, the processes for secure configurations have not been discussed sufficiently, even though security is one of the most important concerns for enterprise applications. Currently, the security properties tend to be ignored until the downstream development phases, and the developers in the downstream phases must manage the configurations. The resulting problems are that the downstream developers do not have sufficient information to create correct configurations and that the configurations themselves are too complex for developers who are not security experts.

This chapter discusses a security configuration process and defines the responsibilities of developers. To configure security correctly, various kinds of information are required, such as business security requirements and platform information. This information is not available at any single downstream development phase, so this chapter defines the developer’s roles from the perspective of the information that is available during each development phase. Thanks to the chapter’s proposed process, all of the developers can concentrate on their own responsibilities for the configuration.

Even if the configuration process is defined clearly, configuring security correctly is quite difficult because SOA security is so complex and the security domain federation must be considered. This chapter also proposes a supporting technology to create concrete configurations: Model-Driven Security. This contributes to generating correct configurations while reducing developers’ workloads.

The remainder of this chapter is structured as follows. The background of and problems in the current configuration processes are discussed in the next section, and then the End-to-End security configuration process is proposed. The supporting technology is discussed; the security configuration process is demonstrated, and related work is discussed.

SOA SECURITY CONFIGURATION PROCESS

Security Domain Federation

The SOA approach develops applications by assembling computing system components called services which may be located on various platforms. These platforms may support their own security technologies, such as Kerberos or PKI, so the different security technologies should be integrated to secure all of the SOA application. This integration is called a security domain federation.

Web Services Security (WS-Security) (Web Services Security, 2006) is one of the security technologies that is typically used for SOA applications. WS-Security proposes a framework for a security federation (IBM and Microsoft, 2002) in which we can integrate various security technologies. Figure 1 shows a typical security federation framework. To exchange secured messages using WS-Security, a requester and a provider should share a common key as a security token. Suppose the service requester provides a username token that includes its own ID and password, but the service provider requests some another kind of token such as a SAML token. The WS-Security federation framework can exchange these different kinds of security tokens using an intermediary server called a security token service (STS). The requester sends a request for a security token exchange and its username token to the STS, and then the STS authenticates the requester and issues the SAML token for the requester to connect to the provider. Then the requester can send a secured message to the provider by using the issued SAML token.
Related Content

Measures for Cloud Computing Effectiveness Assessment
[www.igi-global.com/article/measures-for-cloud-computing-effectiveness-assessment/120244?camid=4v1a](www.igi-global.com/article/measures-for-cloud-computing-effectiveness-assessment/120244?camid=4v1a)

Critical Business Model Issues in Deploying NFC Technology for Mobile Services: Case Mobile Ticketing
[www.igi-global.com/article/critical-business-model-issues-deploying/68828?camid=4v1a](www.igi-global.com/article/critical-business-model-issues-deploying/68828?camid=4v1a)

The Trend Toward Online Banking Services by Brick-and-Mortar Institutions: The Last Five Years
[www.igi-global.com/chapter/trend-toward-online-banking-services/24642?camid=4v1a](www.igi-global.com/chapter/trend-toward-online-banking-services/24642?camid=4v1a)

Protecting Privacy Using XML, XACML, and SAML
[www.igi-global.com/chapter/protecting-privacy-using-xml-xacml/28142?camid=4v1a](www.igi-global.com/chapter/protecting-privacy-using-xml-xacml/28142?camid=4v1a)