Chapter XIII
Providing Web Services Security
SLA Guarantees:
Issues and Approaches

Vishal Dwivedi
Infosys Technologies Limited, India

Srinivas Padmanabhuni
Infosys Technologies Limited, India

ABSTRACT

This chapter underlines the importance of security service level agreements (SLAs) for Web services. As Web services are increasingly incorporated in the mainstream enterprises, the need for security has led to various standards. However, unlike nonfunctional requirements such as performance, scalability and so forth, which are quantitative and are enforced through SLAs, security is represented only through policies. There exist quite a few frameworks for security at different levels of enactment; however, what is clearly missing is an approach to represent security SLAs and enacting them for a Web service environment. In this chapter, we primarily focus on two aspects. We first focus on the security requirements for Web services and the currently available stack of security mechanisms and frameworks for achieving security at various levels of Web service implementation. The second focus is on how these could be utilized to build security SLAs, which could be enforced on Web services. Later in the chapter we suggest a conceptual model to represent these SLA clauses and present an approach to enact them.

INTRODUCTION

The increased adoption of service-oriented architecture (SOA) in enterprise context has drawn attention to nonfunctional aspects as security and privacy. Web services, being the building blocks of SOA,
require service level agreement (SLA) guarantees not only for performance attributes such as reliability and availability but also for other nonfunctional attributes such as security and privacy. The raison d’être for Web services is that they could be used to compose new services. In that sense the conventional notions of “trusted party paradigms” for composition also apply to the Web services. Not only does a secure service composition have to be ascertained but it has to be also ensured that the provider of the Web services could give security SLA guarantees.

In this work we capture some of the security requirements for composition and execution of Web services. We address some of the issues related to security and privacy in the Web services domain, and we discuss some of the current approaches followed to address them. Right from network level security protocols like secure socket layer (SSL), transport layer security (TLS), and so forth, to the SOAP level, and until the federation level security standards, we look at the existing security stacks for Web services. We explore how SLAs are enacted in terms of other nonfunctional requirements like performance and availability and present a mechanism to represent security SLAs. Towards the end we present a conceptual model to represent the security SLAs and an approach to enact them.

BACKGROUND

SLAs have been commonly used to specify nonfunctional requirements which ascertain the criteria for the correct operation of the system. Typical nonfunctional requirements which are covered through SLAs today include reliability, scalability, cost and so forth, most of which are measurable attributes. The need for a Web service security SLA arises from the fact that Web services are designed to be composed from candidate services, the credentials of each required to be verified for an enterprise level service orchestration. A security SLA would typically comprise of the following quality of service (QoS) attributes:

- **Access Control**: Provision of only need-to-know information/privileges.
- **Authorization and Authentication**: The prevention of data/information access by invalid users.
- **Availability**: The prevention of degradation or interruption as a consequence of failures.
- **Confidentiality**: The prevention of unauthorized disclosure of data.
- **Integrity**: The prevention of unauthorized modification of data.

There exist quite a few approaches, standards, and frameworks which address the above issues for implementing security for Web services. Security assertion markup language (SAML) is an XML standard designed by OASIS for exchanging authentication and authorization data between service and identity providers. Not only does it provided support for transport-level security (through SSL 3.0 and TLS 1.0), but it also ensured message-level security (using **XML signature** and **XML encryption**). Later, Liberty alliance extended SAML for identity management. Although SAML was used as a de-facto industry standard for exchanging authorization information, it was limited by its declarative limitations and was followed by extensible access control markup language (XACML), which provided support for a more declarative-access control-policy definition. Later in 2006, W3C defined WS-policy as a XML-based standard for definition and specification of Web services policies (on security and QoS, etc.)
Related Content

Survey Paper on Semantic Web
[www.igi-global.com/chapter/survey-paper-on-semantic-web/217934?camid=4v1a](www.igi-global.com/chapter/survey-paper-on-semantic-web/217934?camid=4v1a)

Event-Driven SOA Based District Heating Service System with Complex Event Processing Capability
Xiuquan Qiao, Budan Wu, Yulong Liu, Zhao Xue and Junliang Chen (2014). *International Journal of Web Services Research* (pp. 1-29).
[www.igi-global.com/article/event-driven-soa-based-district-heating-service-system-with-complex-event-processing-capability/110872?camid=4v1a](www.igi-global.com/article/event-driven-soa-based-district-heating-service-system-with-complex-event-processing-capability/110872?camid=4v1a)

Context and End-User Privacy Policies in Web Service-Based Applications
[www.igi-global.com/chapter/context-and-end-user-privacy-policies-in-web-service-based-applications/214836?camid=4v1a](www.igi-global.com/chapter/context-and-end-user-privacy-policies-in-web-service-based-applications/214836?camid=4v1a)

A Novel Freeway Traffic Speed Estimation Model with Massive Cellular Signaling Data