Chapter IX

Dynamic, Flow Control-Based Information Management for Web Services

Zahir Tari, RMIT University, Australia
Peter Bertok, RMIT University, Australia
Dusan Simic, RMIT University, Australia

Abstract

Information Flow Control (IFC) is a method of enforcing confidentiality by using labels, data structures for specifying security classifications. IFC is used in programming languages to monitor procedures in an attempt to detect and prevent information leakage. While it ensures greater security, IFC excessively restricts flow of information. This chapter presents a model of information flow control using semi-discretionary label structures. We propose a set of rules that not only increase the flexibility of IFC, but also define labels as a practical component of a security system. We propose a dynamic approach using a centralized model for dynamic label checking, and verify the proposed model using theoretical proofs.

Introduction

Web services have greatly improved the way businesses deal with transactions over the Internet. One of their attractive features is that they operate in a loosely coupled way that facilitates their cooperation and makes them flexible. This advantage, however, comes with some drawbacks—for example, restrictions on access to data are difficult to enforce. Information leak, also called declassification, is a growing concern, as Web services handle customer data that include highly sensitive information. The possibility of unauthorized access to data can affect several aspects of Web service security. Confidentiality of data can be compromised—for example customer credit card data can be accessed by criminals. Privacy breaches also become possible, when data is used for purposes other than those the data was provided for, such as leaking health records of a person.

Several standards have been developed to enhance Web service security. XML Encryption (W3C, 2002a) and XML Signature (W3C, 2002b) are for securing communication. SAML (OASIS, 2005) is designed to facilitate authentication and authorization via exchanging security assertions. In a typical example an SAML message describes that a particular subject has been authenticated by a certain method at a given point in time, or if a subject is allowed to access a particular resource. While SAML provides a mechanism to exchange such security assertions, it is not concerned with establishing or enforcing them; it is the responsibility of the communicating partners to define the security features and implement the relevant mechanisms.

Proposed Approach

In this chapter we propose information flow control as the means to prevent information leakage and declassification. Access to information is controlled by the system, whose modules are distributed, and each participant carries the access control logic that must be applied when handling data. Security labels attached to objects carry information about the sensitivity of the data and describe accessibility. The only way to retrieve or update data is through special modules or plug-ins that are part of the communication infrastructure. The modules check flow legality and administer access rights in a distributed manner.

The approach is suitable to any message-exchange-based system. Our solution uses XML description that suits the XML-SOAP environment of Web services well.