Chapter 5.19
Model Driven Security for Inter-Organizational Workflows in E-Government

Michael Hafner
Universität Innsbruck, Austria

Barbara Weber
Universität Innsbruck, Austria

Ruth Breu
Universität Innsbruck, Austria

Andrea Nowak
Austrian Research Center Seibersdorf, Austria

ABSTRACT

Model driven architecture is an approach to increase the quality of complex software systems by creating high-level system models and automatically generating system architectures and components out of these models. We show how this paradigm can be applied to what we call model driven security for inter-organizational workflows in e-government. Our focus is on the realization of security-critical inter-organizational workflows in the context of Web services, Web service orchestration, and Web service choreography. Security requirements are specified at an abstract level using UML diagrams. Out of this specification security, relevant artifacts are generated for a target reference architecture based on upcoming Web service security standards. Additionally, we show how participants of a choreography use model dependencies to map the choreography specifications to interfaces for their local workflows.

INTRODUCTION

E-government refers to the use of the Internet and other electronic media to improve the collaboration within public agencies and to include citizens and companies in administrative processes. A core aim of e-government is to bring about a digital administration in order to enhance quality of service (e.g., additional online information or service offerings) as well as efficiency (e.g., reduced case processing times, fewer errors or using fewer resources to accomplish the same task).

The implementation of e-government solutions is a very complex task that can only succeed if IT-experts and domain experts cooperate with each other at a high level of abstraction right from the beginning. Security issues rooted in provisions and regulations play a very critical role. These include security requirements of public law (i.e., Austrian Signature Act [1999] and the Austrian e-government Act [2004] as well as the Federal Act concerning the Protection of Personal Data [1999]), the Austrian Security Manual [n.d.], the OECD Guidelines for the Security of Information Systems and Networks [n.d.], and internal security requirements of the municipalities.

Security requirements must not be considered as an isolated aspect, except during all stages of the software development cycle (Devanbu & Stubblebine, 2000; Ferrari & Thuraisingham, 2000). As the engineering of security into the overall software design is often neglected, different approaches for integrating security in the system development cycle have been proposed (Hall & Chapman, 2002; Breu, Burger, Hafner, & Popp, 2004). Nevertheless, they do not yet exploit the potential of a model driven approach.

Model driven software development is particularly appealing in the area of security as many security requirements adhere to certain categories (e.g., integrity) and can be described in implementation-independent models. In most cases, the development of security-critical systems is based on a set of well-known protective measures (i.e., protocols, algorithms) for which the correctness has been proved.

In this chapter, we give an overview of our approach to the model driven realization of security-critical inter-organizational workflows in the context of Web services security, Web service orchestration, and Web service choreography. The description of security requirements is performed at a high level of abstraction. Security relevant artifacts are generated for a target architecture. A description of the target architecture can be found in Hafner, Breu, and Breu (2005) and Brue, Hafner, and Web (2004).

Our approach provides a specification framework for the design of collaborating systems in the context of the platform-independent Web service technology. It also supports the systematic transition from security requirements, via the generation of security artifacts, to a secure solution based on a Web services platform. The specification of security requirements is performed in a platform-independent way and can thus be applied by domain experts without in-depth technical knowledge.

The structure of the subsequent sections is as follows. After providing an overview on Web services composition, Web services security, and Model Driven Architecture in Section 2, we present a case study in Section 3, and describe our model driven approach in Section 4. In Section 5, we describe our component-based Target Reference Architecture. Finally, Section 6 gives an overview of related work before Section 7 closes with a conclusion.

Backgrounds

This section briefly sketches the standards, technologies, and methodologies our approach is based upon.

Web Services Standards

The growing popularity of emerging Web services standards and technologies pushes the specification and implementation of powerful infrastructures based on platform-independent technology. The goal is to foster interoperability