Chapter 14


Sven Feja
Christian-Albrechts-University of Kiel, Germany

Sven August
Christian-Albrechts-University of Kiel, Germany

Andreas Speck
Christian-Albrechts-University of Kiel, Germany

Meiko Jensen
Ruhr-University Bochum, Germany

Jörg Schwenk
Ruhr-University Bochum, Germany

ABSTRACT

An increasing need for security in SOA applications demands for better support for the management of security in Web-based business processes. Here, the model-driven process development may provide valuable opportunities in terms of maintainability and deployment. Besides modeling and then generating the pure functionality of a process, the consideration of security properties at the level of a process model allows us to derive appropriate Web Service security policies as well. Especially important when dealing with security issues is the need of trust in the deployed processes and the development process as well.

In this chapter, the authors discuss the general capabilities and constraints for model-driven security. Furthermore, the authors focus on the automatic transformation of security models into executable security implementations as well as on the validation of the security models to ensure their correctness. Based on the discussion, the authors present a transformation mechanism that automatically derives WS-SecurityPolicy-conformant security policies. Moreover, the chapter presents a validation mechanism for the security model which is based on graphical validation rules. The application of both mechanisms allows the automatic deployment of validated, security-enabled Web Service based business processes.

DOI: 10.4018/978-1-4666-0146-8.ch014
INTRODUCTION

Model-driven software development (MDSD) (e.g. realized by the Model-Driven Architecture (MDA) (The Object Management Group, 2003)) intends to provide a more efficient development of complex software applications. The basis of MDSD is a model, which gets stepwise refined and transformed into an executable software product. In the domain of e-business different types of models are used to describe business processes, e.g. UML activity diagrams, event-driven process chains (EPC) (Keller, Nüttgens, & Scheer, 1992) or BPMN diagrams (The Object Management Group, 2006). Besides the type of model, the modeling tools and their capabilities are an important factors while applying the MDSD process.

A tool which intends to support the MDSD process mainly has to fulfill two tasks—the modeling of processes and the transformations of high level process model to the executable process or source code. A model, that can be used as basis for the MDSD, needs to be enriched with a lot of properties. This includes the high level business requirements as well as specific details for the implementation. Therefore, a modeling and MDSD tool respectively should be able to show only the information important to a specific stakeholder—each as a separate view. As Lübke, Lüecke, Schneider, & Gómez (2008) states, this is a challenging service, which should be provided by any MDSD tool.

Next to the need of different views, the modeling capabilities of a modeling notation have to be considered. This reveals that the modeling e.g. of security properties is not commonly provided by a modeling notation as well as by a MDA tool. For instance, the modeling of security properties often is supported unsatisfactorily (see section "Existing Security Modeling Capabilities"), though security aspects are an essential issue for many domains. In electronic business, an obvious scenario is an online business process where specific information like credit card data needs to be kept secret.

Technically, MDA implementations of electronic business processes are often realized on the basis of the Web Services platform architecture (Weerawarana, Curbera, Leymann, Storey, & Ferguson, 2005). Web Services are a realization of the service-oriented architecture paradigm (SOA) (MacKenzie, Laskey, McCabe, Brown, & Metz, 2006), which gained broad attention (especially for MDSD) in science and industry. Particular advantages of the Web Services technology are their broad industrial support, high interoperability, and a well-defined abstraction layer approach.

Especially, the broad industrial support has resulted in comprehensive standardization activities. Therefore, today most of the aspects related to Web Services are defined by a standardized specifications. This includes e.g. data representation, transaction management, reliability and security. For example, the handling of important security properties (e.g. for electronic business processes) like authentication, access control, data integrity, and confidentiality are defined by these standards.

In this chapter, we investigate the MDSD approach which uses business process models which are transformed into executable process descriptions (WS-BPEL (Jordan et al., 2007)) and WSDL-based Web Service realizations. Based on this investigation, we present an extension to the MDSD approach which allows the specification of security requirements within a business process model. As an exemplary modeling notation, we use EPCs to illustrate our approach. The extended EPC—a security model—is transformed automatically (according to (Jensen & Feja, 2009)) into an appropriate representation for the Web Services platform. Primarily, we discuss the possibility of denoting the security properties of confidentiality, data integrity, and access control in EPC models, which then are mapped to security policies (WS-SecurityPolicy specification (Kaler & Nadalin, 2005)) for the underlying Web Services. The security model can be realized as a security view for a modeling tool like the ARIS...