SecureBPMN: Modeling and Enforcing Access Control Requirements in Business Processes

Achim D. Brucker
SAP Research
Vincenz-Priessnitz-Str. 1
76131 Karlsruhe, Germany
achim.brucker@sap.com

Isabelle Hang
SAP Research
Vincenz-Priessnitz-Str. 1
76131 Karlsruhe, Germany
isabelle.hang@sap.com

Gero Lückemeyer
Hochschule für Technik Stuttgart
Schellingstr. 24
70174 Stuttgart, Germany
gero.lueckemeyer@hft-stuttgart.de

Raj Ruparel
SAP Research
Vincenz-Priessnitz-Str. 1
76131 Karlsruhe, Germany
raj.ruparel@sap.com

ABSTRACT

Modern enterprise systems have to comply to regulations such as Basel III resulting in complex security requirements. These requirements need to be modeled at design-time and enforced at runtime. Moreover, modern enterprise systems are often business-process driven, i. e., the system behavior is described as high-level business processes that are executed by a business process execution engine.

Consequently, there is a need for an integrated and tool-supported methodology that allows for specifying and enforcing compliance and security requirements for business process-driven enterprise systems.

In this paper, we present a tool chain supporting both the design-time modeling as well as the run-time enforcement of security requirements for business process-driven systems.

Categories and Subject Descriptors

K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems—*Security and Protection*

General Terms

Security, Languages

Keywords

Process Security, SecureBPMN, RBAC, BPMN

1. INTRODUCTION

Security requirements and compliance regulations are a major concern for designing, building, and running business process driven systems. Many software development methods often treat non-functional requirements, such as security, separately. As the functional behavior and the security of a system are, usually, not independent from each other, this separation of concerns makes it difficult to ensure that a given system fulfills its requirements. Thus, we propose a tool supported, model-driven development process that integrates seamlessly the security and compliance requirements across all phases of the system life-cycle, i. e., from the *system design* to *system execution* to *system audit.*

In this paper, we concentrate on the first two aspects: integrating security and compliance requirements into a BPMN-based design phase as well as enforcing these requirements, at run-time, in a workflow management system.

2. THE SECUREBPMN METHODOLOGY

Consider a travel approval process in which the budget and the travel duration need to be approved by different managers. The main window in Figure 1 illustrates such a process. This simple process requires already the following compliance and security requirements (see, e. g., [10] for a more detailed discussion of security requirements for process models):

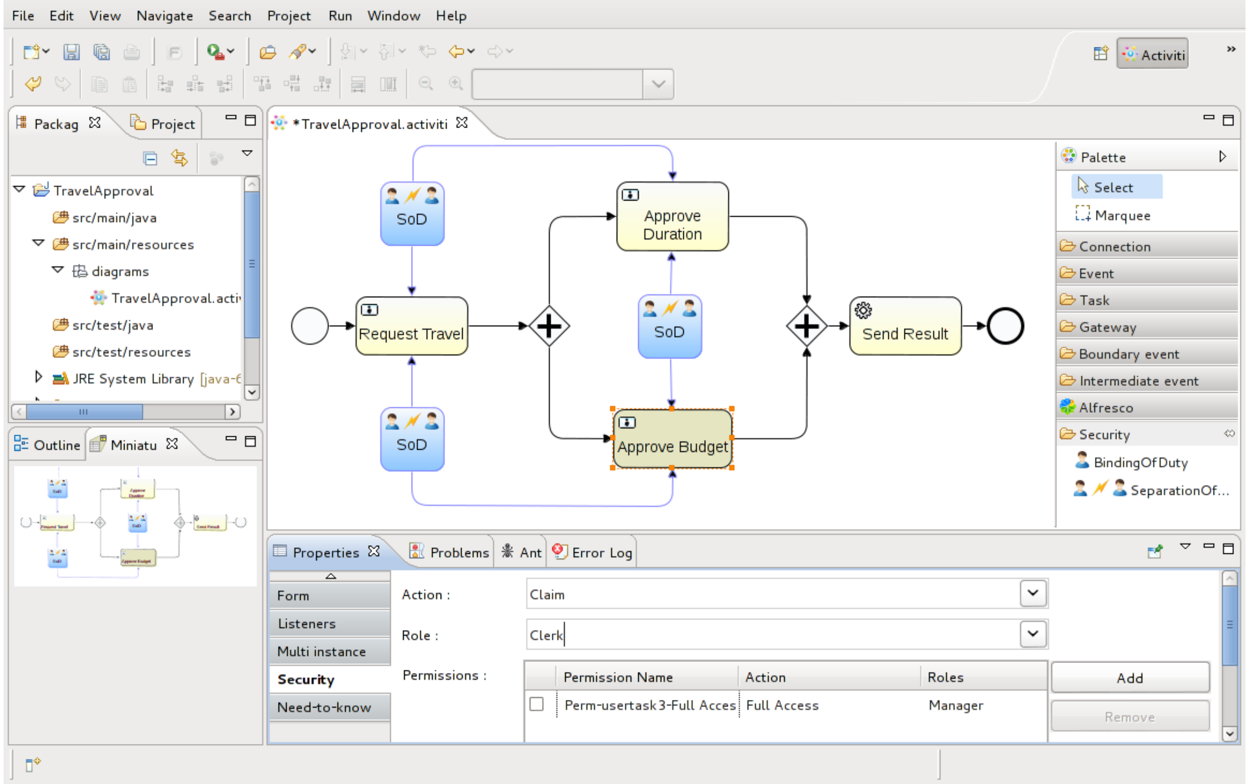
- *Access Control:* Access to resources as well as actions need to be restricted to certain roles (e. g., clerks, managers) or subjects.
- *Separation of Duty:* More than one subject is required to successfully complete the process.

While modeling several other case studies we identified the following security requirements as particularly important:

- *Binding of Duty:* The same subject needs to execute several tasks of a process.
- *Need to Know:* A subject should only be able to access the information that is strictly necessary for completing a certain task.

In the following, we discuss how these requirements can be modeled and enforced for business-process-driven systems.

.



Action : Claim

Role : Clerk

Permissions :

	Permission Name	Action	Roles
□	Perm-usertask3-Full Acces	Full Access	Manager

Figure 1: Specifying security requirements diagrammatically as well as using specialized user interfaces.

2.1 Modeling Security Requirements

Modeling compliance and security requirements on the process level requires the extension of the process modeling language with security concepts. In our work, we follow the meta-modeling approach for extending the Business Process Modeling and Notation (BPMN) [9] with a security language, called SecureBPM, that allows for specifying role-based access control (RBAC) [1] as well as the other security and compliance properties. The decision for a meta-model based approach is based on our previous experience in extending UML with RBAC (see [4] for a comparison of the different possibilities for adding domain-specific extensions to an existing modeling language).

Beside the specification of hierarchical, role-based access control (inspired by SecureUML [3]), SecureBPMN supports, e. g., separation of duty and binding of duty constraints. In contrast to standard approaches, our meta-model allows to specify these requirements not on the task level but on the permission level. This supports use cases where separation of duty or binding of duty is only necessary under certain conditions, e. g., the travel request has to be approved by two managers or one senior manager.

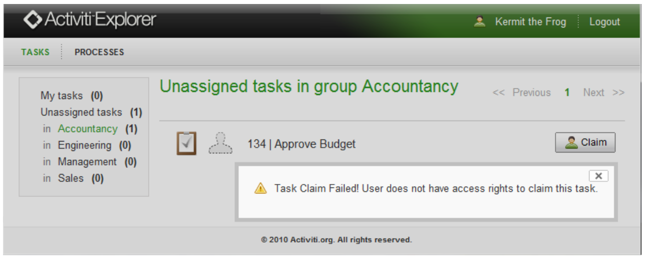
Moreover, SecureBPMN also supports the need-to-know principle which restricts the use of resources such as process variables or data objects.

The visualization of these security requirements is another characteristic of our work. They must be embedded in a business process model during the BPMN-based design phase in a well-arranged manner. So, we provide diagrammatic representations as well as specialized user interfaces to avoid crowded diagrams. We decide to depict separation of duty and binding of duty in a diagrammatic way and specify access control and need to know in a domain-specific user interface.

2.2 Enforcing Security Requirements

Naturally, the specified security and compliance requirements need to be enforced at runtime. Integrating security requirements, as first-class citizen, into the process modeling language, allows to easily support modern service-oriented or cloud-based systems. In contrast to traditional monolithic workflow systems, modern systems are usually a composition of many different services and each of these services needs to enforce a subset of the security requirements. Moreover, there are requirements, e. g., separation of duty, that need to be enforced by the workflow management system orchestrating the various services.

To address this challenge, we propose to apply the Model-driven Security (MDS) paradigm, i. e., to generate the necessary artifacts for standard security frameworks from the SecureBPMN model. Generating these artifacts allows for generating all the security configuration for all services from a *single* source—even for services using different security frameworks. For example, the RBAC, separation of duty, and binding of duty requirements can be automatically translated into XACML [8] policies and enforced by one or more Policy Enforcement Points (PEPs). The PEPs are generated from the SecureBPMN model as well and use an XACML Policy Decision Point (PDP) to decide if a certain request should be granted or not. If a request is denied, the PEP in the user interface of the workflow management systems informs the user about the violation of the security policy.



Unassigned tasks in group Accountancy

134 | Approve Budget

Task Claim Failed! User does not have access rights to claim this task.

© 2010 Activiti.org. All rights reserved.

Figure 2: Enforcing SecureBPMN policies at run-time and informing users about violations.

2.3 Implementation

Our prototype uses the Activiti BPMN Platform (`http://www.activiti.org/`). In particular, we extended the Activiti Eclipse Designer and the Activiti Process Engine.

Our extension of the Activiti Designer provides an integrated environment for modeling secure business processes. As we made the experience that many security requirements are too complex to be represented intuitively in a diagrammatic way, we provide diagrammatic extensions of BPMN as well as security specific extension of the user interface:

- For certain requirements, such as separation of duty, we provide a diagrammatic representation, i. e., user can specify separation of duty constraints via drag using the Palette (see the right-hand side of Figure 1),
- For the specification of the role-based access control policies as well as certain details of, e. g., complex separation of duty constraints, we provide specialized user interfaces. For example, the Security Tab for tasks (see the lower part of Figure 1) allows for a table-based specification of access control requirements.

The diagrammatic representation of security requirements and the security-specific user interfaces are two views on the same secure process model. Thus, the user is free to choose the specification approach that best suits his or her needs.

For the access control enforcement, we automatically generate XACML policies as well as XACML compliant PEPs based on SUN's XACML implementation (`http://sunxacml.sf.net/`). Of course, support for other policy languages can be added easily. Moreover, we extended the Activiti Process Engine to use the generated PEPs for enforcing the security policies as well as informing users about certain violations, e. g., the violation of a separation of duty constraint (see Figure 2).

3. CONCLUSION AND FUTURE WORK

We presented a model-based approach for designing and operating business-process-driven systems that integrates security and compliance requirements as first class citizens.

In this paper, we concentrated on the design-time modeling as well as the run-time enforcement of security and compliance requirements. Providing an integrated solutions that ensures the secure and compliant operation of business-process-driven systems, requires, requirements, further extensions in several ways. For example, at design-time we plan to integrate consistency analysis techniques similar to [2] as well as formal security analysis techniques such as [6].

Moreover, the use of model-based test case generation techniques, e. g., similar to [7], allows for ensuring that, on the one hand, access control enforcement infrastructure works correctly and, on the other hand, that externals services adhere to the security requirements as well. Finally, we suggest to integrate policy analysis frameworks such as [5] to cover the system audit phase.

Acknowledgments.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007–2013) under grant no. 257930 (Aniketos).

References

[1] *American National Standard for Information Technology – Role Based Access Control.* ANSI, New York, 2004. ANSI INCITS 359-2004.

[2] W. Arsac, L. Compagna, G. Pellegrino, and S. E. Ponta. Security validation of business processes via model-checking. In Ú. Erlingsson, R. Wieringa, and N. Zannone, editors, *ESSoS*, volume 6542 of *LNCS*, pages 29–42. Springer, 2011. doi: 10.1007/978-3-642-19125-1_3.

[3] D. A. Basin, J. Doser, and T. Lodderstedt. Model driven security: From UML models to access control infrastructures. *ACM Transactions on Software Engineering and Methodology*, 15(1):39–91, 2006. doi: 10.1145/1125808.1125810.

[4] A. D. Brucker and J. Doser. Metamodel-based UML notations for domain-specific languages. In J. M. Favre, D. Gasevic, R. Lämmel, and A. Winter, editors, *4th International Workshop on Software Language Engineering (ATEM 2007)*. 2007.

[5] A. D. Brucker and H. Petritsch. A framework for managing and analyzing changes of security policies. In *IEEE POLICY*, pages 105–112. IEEE Computer Society, 2011. doi: 10.1109/POLICY.2011.47.

[6] A. D. Brucker, J. Doser, and B. Wolff. A model transformation semantics and analysis methodology for SecureUML. In O. Nierstrasz, J. Whittle, D. Harel, and G. Reggio, editors, *MoDELS 2006: Model Driven Engineering Languages and Systems*, number 4199 in LNCS, pages 306–320. Springer, 2006. doi: 10.1007/11880240_22.

[7] A. D. Brucker, L. Brügger, P. Kearney, and B. Wolff. An approach to modular and testable security models of real-world health-care applications. In *ACM SACMAT*, pages 133–142. ACM Press, 2011. doi: 10.1145/1998441.1998461.

[8] OASIS. eXtensible Access Control Markup Language (XACML), version 2.0, 2005.

[9] Object Management Group. Business process model and notation (BPMN), version 2.0, 2011. Available as OMG document formal/2011-01-03.

[10] A. Rodríguez, E. Fernández-Medina, and M. Piattini. A BPMN extension for the modeling of security requirements in business processes. *IEICE - Trans. Inf. Syst.*, E90-D:745–752, 2007. doi: 10.1093/ietisy/e90-d.4.745.