Integrating BPMN- and UML-based Security Engineering via Model Transformation

Qusai Ramadan[1], Mattia Salnitri[2], Daniel Strüber[3], Jan Jürjens[4], Paolo Giorgini[5]

Keywords: model-driven security; security by design; BPMN; UML; model transformation

1 Abstract

We present our paper from the proceedings of the 2017 edition of the IEEE/ACM International Conference on Model-Driven Engineering Languages and Systems (MODELS) [Ra17].

Most software systems today are embedded into Socio-Technical Systems (STSs), in which organizational and technical components are coordinated to accomplish shared objectives. Establishing security is particularly challenging in STSs since security issues may be propagated along these components, which are generally autonomous and hard to control. Previous work supports the management of organizational and technical security requirements in the early stages of the development process. *BPMN-based approaches* such SecBPMN2 [SDG14] abstract from technical details to support business analysts in specifying organizational security requirements as part of business processes for the target STS. *UML-based approaches* such as UMLsec [Jü05] support system developers in specifying technical security requirements and security-related assumptions in architectural models. The resulting models can be validated against pre-defined technical security policies.

Since these existing BPMN- and UML-based approaches address security in distinct development phases and from distinct stakeholders' perspectives, they deal with security requirements separately; vulnerabilities may arise from misunderstandings between these stalkeholders, in particular due to the divergent use of terminology. For instance, without the knowledge that BPMN's *swimlanes* are commonly used to express internal roles in an organization, a system developer may forgo the use of an appropriate role enforcement mechanism. Such loopholes may be hard to detect, since traceability mechanisms for security requirements across the different phases are usually not available.

[1] Universität Koblenz-Landau, Universitätsstr. 1, 56070 Koblenz, Germany, qramadan@uni-koblenz.de

[2] University of Trento, Via Sommarive 9, I-38050, Povo (Trento) Italy, mattia.salnitri@unitn.it

[3] Universität Koblenz-Landau, Universitätsstr. 1, 56070 Koblenz, Germany, strueber@uni-koblenz.de

[4] Universität Koblenz-Landau, Universitätsstr. 1, 56070 Koblenz, Germany and Fraunhofer Institute for Software and Systems Engineering, Emil-Figge-Str. 91, 44227 Dortmund, Germany, juerjens@uni-koblenz.de

[5] University of Trento, Via Sommarive 9, I-38050, Povo (Trento) Italy, paolo.giorgini@unitn.it

To address these issues, we propose a framework for designing secure STSs by integrating existing BPMN-based and UML-based security engineering approaches. Our framework involves four main tasks: (i) Organizational security requirements are modeled by business analysts using SecBPMN2, (ii) the SecBPMN2 model is transformed to a preliminary UMLsec-annotated architectural model automatically, using a Henshin-based model transformation [St17], (iii) the generated UMLsec model is manually refined by system developers, and (iv) the resulting UMLsec model is verified against the contained security policies automatically using a tool called CARiSMA [Ah17].

The main contributions of the current paper are:

- a *semi-automated process* that enforces security management throughout the development process in an integrated manner,
- a *model transformation* that supports the translation of security-annotated business models to security-annotated architectural models while establishing traceability, and
- a *case study* featuring an air traffic management system, in which our framework was used to establish integrated management and traceability of security requirements.

Our framework automatically establishes traceability between high-level security requirements and verifiable technical security policies. Doing so, it integrates the perspectives of business analysts and system developers, the main expert stakeholders in STS development.

An accompanying artifact for our paper (`http://www.remodd.org/v1/content/models2017-bpmn2uml-artifacts`) was accepted at MODELS's Artifact Evaluation track.

References

[Ah17] Ahmadian, Amir Shayan; Peldszus, Sven; Ramadan, Qusai; Jürjens, Jan: Model-based privacy and security analysis with CARiSMA. In: Joint Meeting on Foundations of Software Engineering (ESEC/FSE). pp. 989–993, 2017.

[Jü05] Jürjens, Jan: Secure systems development with UML. Springer Science & Business Media, 2005.

[Ra17] Ramadan, Qusai; Salnitri, Mattia; Strüber, Daniel; Jürjens, Jan; Giorgini, Paolo: From Secure Business Process Modeling to Design-Level Security Verification. In: ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS). pp. 123–133, 2017.

[SDG14] Salnitri, Mattia; Dalpiaz, Fabiano; Giorgini, Paolo: Modeling and verifying security policies in business processes. In: Enterprise, Business-Process and Information Systems Modeling (BMMDS/EMMSAD), pp. 200–214. Springer, 2014.

[St17] Strüber, Daniel; Born, Kristopher; Gill, Kanwal Daud; Groner, Raffaela; Kehrer, Timo; Ohrndorf, Manuel; Tichy, Matthias: Henshin: A Usability-Focused Framework for EMF Model Transformation Development. In: International Conference on Graph Transformation (ICGT). pp. 196–208, 2017.