Master / Bachelor

Ableitung von Sicherheits- und Privacy-Anforderungen aus secBPMN Modellen

Eliciting textual security and privacy requirements from secBPMN models

Kontakt / Contact

M.Sc. Katharina Großer (grosser@uni-koblenz.de)

Deutsch: (For English see p. 2)

Motivation

Business Process Model and Notation (BPMN) ist eine weit verbreitete Modellierungssprache zur Darstellung von Geschäftsprozessen. BPMN kann als Kommunikationsbasis während der Anforderungserhebung dienen oder als semi-formale notation, um diese Anforderungen zu erfassen. Die Formalisierung der Prozesse kann verstecktes Wissen freilegen, z.B. unbekannte Akteure, Verantwortlichkeiten und Systemgrenzen. Basierend auf dieser Hypothese ist es sinnvoll mit der Definition der Prozesse zu beginnen, um sicherzustellen, dass das entwickelte System den Bedürfnissen der Kunden entspricht.

Jedoch setzt das Lesen und Verstehen der Modelle Wissen über die Notation voraus, was nicht bei allen Beteiligten gegeben ist. Natürlichsprachliche Anforderungen sind für alle Beteiligten ohne weiteres Training verständlich, insbesondere auch für solche, die nicht direkt an der Entwicklung beteiligt sind, aber Teil des Projektmanagements sind, wie etwas juristische Berater. Außerdem können nicht alle Anforderungen in Prozessmodellen ausgedrückt werden. Insbesondere nicht-funktionale Anforderungen werden in State-of-the-art Prozessmodellierungsmethoden unzureichend unterstützt. Für die meisten Projekte ist es daher notwendig ein erweitertes vollständiges natürlichsprachliches Anforderungsdokument zu erstellen, welches zu den Prozessmodellen konsistent ist.

Es existieren Ansätze die Ableitung funktionaler Anforderungen aus BPMN-Prozessmodellen zu formalisieren. Dabei führt die Verwendung von Anforderungs-Templates zu qualitativ hochwertigen Anforderungen in strukturierter Sprache. Dies erzeugt nicht nur Anforderungen höherer Qualität, sondern es ermöglicht auch ein eindeutiges Mapping zwischen beiden Notationen und die Sicherstellung der Konsistenz.

secBPMN erweitert BPMN um Sicherheits-Annotationen und es existiert weiterhin eine Erweiterung zu Privacy. Ziel dieser Arbeit ist es existierende Ansätze zur Anforderungserhebung aus BPMN-Modellen um Sicherheits- und Privacy-Anforderungen zu erweitern.

Aufgabenstellung/Ziele

Ziel ist es Ableitungsregeln zu definieren, um textuelle Sicherheits- und Privacy-Anforderungen in strukturierter Form aus secBPMN-Modell zu erheben und ein entsprechendes Tool zur Anforderungsdefinition zu erweitern.

Zu den Aufgaben gehört:

- Identifikation verschiedener Arten von Sicherheits- und Privacy-Anforderungen in secBPMN-Annotationen
- Definition von Ableitungsregeln:
  - Mapping zwischen identifizierten Anforderungstypen und Templatetypen

  - Mapping von (sec)BPNM-Elementen zu Template-Elementen
  - ggf. Erweiterung der Templates
- Implementation des Imports von secBPMN-Modellen in existierendes Tool
- Implementation der neuen Ableitungsregeln im Tool
- Evaluation der Ableitungsregeln und der Implementation

Hilfreiche Vorkenntnisse

Der/die Kandidat/in sollte die Vorlesung Grundlagen der Softwaretechnik (ggf. auch Vertiefung der Softwaretechnik) erfolgreich absolviert haben. Außerdem sind hilfreich:

- Erfahrungen im Requirements Engineering oder die Bereitschaft sich entsprechend einzuarbeiten
- Erfahrungen mit BPMN oder die Bereitschaft sich entsprechend einzuarbeiten
- Interesse an innovativen Technologien des Software Engineerings
- Grundkenntnisse in IT-Sicherheit (Vorlesung IT-Sicherheit) oder die Bereitschaft sich entsprechend einzuarbeiten
- Erfahrungen mit HTML, CSS, JavaScript, XML, XQuery, XPath und BaseX hilfreich
- LaTeX-Kenntnisse

English:

Motivation

The Business Process Model and Notation (BPMN) is widely used to model business processes. It can thus serve as a communication basis during elicitation or as a semi-formal notation to document the respective requirements. The formalization of processes reveals hidden knowledge, e.g. unknown actors, and helps to identify responsibilities and system boundaries. Based on this hypothesis, developing a software that fits the customer's needs should start with engineering their processes.

Nevertheless, modeling or even only understanding business process models requires knowledge of the respective notation, that is not always given for all domain experts involved in the requirements elicitation. Natural language requirements are comprehensible for all stakeholders without additional training. This is particularly important for stakeholders not involved in the development process itself but being part of the project management, e.g. legal advisers. Furthermore, not all requirements, can be expressed in process models. Especially for non-functional requirements there is only very limited support in state-of-the-art business process modelling. Therefore, for most projects there is a need to finally maintain an extended set of textual requirements consitent with the requirements expressed business process models.

There exist methodologies to formalize the requirements elicitation process for functional requirements starting from BPMN process models. The usage of requirement templates leads to a set of well-formed and structured natural language requirements. Not only does this increase the quality of textual requirements, it also enables a distinct mapping of elements between both notations and to ensure consistency.

The secBPMN notation and its extension for privacy annotates BPMN model with additional security and privacy constraints. The goal of this thesis is to extend the existing methodology to elicit privacy and security requirements from such annotated models.

Tasks/Goals

The goal of this thesis is to define derivation rules to elicit textual security and privacy requirements from secBPMN models in a structured formal way.

Tasks are:

- Identification of different security and privacy requirements types in secBPMN
- Definition of derivation rules:
  - Mapping between identified types and template types
  - Mapping of (sec)BPMN elements to template elements
  - potentially extension of template definitions
- Implementation of secBPMN import to existing tool
- Implementation of new derivation rules
- Evaluation of rules and tool

Helpful Precognition

The candidate should have passed at least a basic course in software technology. Furthermore:

- Experience in requirements engineering or the willingness to become acquainted
- Basic knowledge with BPMN or the willingness to become acquainted
- Interest in innovative software engineering technologies
- Basic knowledge of IT security and privacy (lecture IT security) or the willingness to become acquainted
- Experience with HTML, CSS, JavaScript, XML, XQuery, XPath, and BaseX helpful
- Knowledge in LaTeX