Security and Compliance Requirements Enforcement for Business Processes

Master thesis

Supervisors: Prof. Dr. Alexander Pretschner, Mohsen Ahmadvand, Amjad Ibrahim
Email: {pretschn, ahmadvan, ibrahim} @ in.tum.de
Phone: +49 89 289 – 17, 314
Starting date: immediately

Context

A business process consists of a workflow of activities, a set of security requirements and a set of business compliances that pursues a specific goal. Processes can either be developed statically (business logic hardcoded in an application) or modelled by the end user and executed dynamically by a workflow engine, e.g. Oracle BPM12c or jBPM2.

Service oriented architecture has significantly motivated the use of process modelling approaches. While services are developed distinctly (and often owned by different parties), businesses can readily orchestrate those services according to their needs. This is extremely powerful in defining complex business needs. However, within such a dynamic context, complying with changing security and business requirements quickly becomes a problem.

Goal

The goal of this thesis is to design and implement a security and compliance monitoring and enforcement mechanism for processes defined in Business Process Modelling Notation (BPMN). At first, a domain specific policy language is adopted to augment the BPMN specification with security and compliance requirements. Later on, these requirements are transformed to a set of policies and stored in a Policy Decision Point (PDP). Finally, a Process Enforcement Point (PEP) is developed (or adopted) to enforce respective policies at runtime.

The second goal of this thesis is to perform a case-study on a real-world software solution offered by Brainloop3, which has agreed to be the industrial partner for this thesis topic. This case-study will include a) integration of the policy enforcement mechanism, b) security evaluation of the implemented mechanism and c) performance evaluation of the mechanism.

1 http://www.oracle.com/us/technologies/bpm
2 http://www.jbpm.org/
3 http://www.brainloop.com/
Workplan

1. Write state-of-art survey of several compliance and security enforcement techniques for business processes.
2. Implement a mechanism for BPMN specified processes, monitoring and enforcement in Go.
   a. Choose one or more compliance and security enforcement technique through a coherent argumentation, i.e. security versus performance, which must be presented in written form.
      i. At very least access control security measures must be modelled
   b. Augment BPMN modelling tool such that security and compliance requirements could be added to any BPMN model.
   c. The design & implementation decisions must be documented in written form.
   d. Policy decisions and enforcement can be implemented using PDP, PEP libraries developed by former students.
3. Case-study on real-world software solution
   a. Integration of the mechanism into the existing process engine
   b. Security evaluation of the developed mechanism in the context of the system, using threat analysis.
   c. Performance evaluation of the mechanism including memory and runtime overhead
4. The final thesis document must contain:
   a. Description of the problem and motivation
   b. Description of the theoretical background
   c. Implementation description
   d. Performance evaluation of implementation and protected programs
   e. Security evaluation of protected programs
   f. Conclusions and future work.

Deliverables

- Virtual machine able to run a demo of the implementation, including instructions on how to run the demo.
- The VM should also include the source code of the implementation.
- Technical report with comprehensive documentation of the implementation, i.e. design decision, architecture description, API description and usage instructions.
- Final thesis report written in conformance with TUM guidelines.

References