Reasoning over Secure Business Processes

Achim D. Brucker
achim.brucker@sap.com
joint work with Luca Compagna, Pierre Guilleminot, and Isabelle Hang

SAP AG, Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany
Dagstuhl Seminar 13211: “Automated Reasoning on Conceptual Schemas”
http://www.dagstuhl.de/13211
19.05.2013 – 24.05.2013
Abstract

Modern enterprise systems are often process-based, i.e., they allow for the direct execution of business processes that are specified in a high-level language such as BPMN.

We present an approach for validating the compliance of the business processes during design-time. Basically, while modeling a business process the business analyst specifies as well the security and compliance requirements the business process should comply to. By pressing a button, these requirements are validated and the results are presented in a graphical format to the business analysis. As proof-of-concept we created a prototype in which the SVaaS Server is deployed on the SAP NetWeaver Cloud and two SVaaS Connectors are built to enable two well-known BPMN tools, SAP NetWeaver BPM and Activiti, to consume SVaaS against industrial relevant business processes.
• Access Control
• Delegation
• Separation/Binding of Duty
• Need to Know
• Break Glass
What and Where to Check

What to Check

• Structural issues
  • deadlocks
  • ...
• Compliance issues
  • need to know
  • separation of duty
  • binding of duty
  • data confidentiality
  • ...
• Security issues
  • access control
  • ...

Where to Check

• Process level
  • consistency of security specifications
  • static vs. dynamic enforcement
  • ...
• Implementation level
  • access control infrastructure
  • data flows (confidentiality)
  • ...

How to Check

• Model checking
• Theorem proving (e.g., SMT)
• Static code analysis
Security Validation of Business Process

- Express security requirements
- Detect vulnerabilities at design time
- Highlight execution paths leading to a security violation so to provide guidelines in solving the problem
- Mitigate the deployment of non-compliant business processes
A Cloud-based Architecture

[Diagram of cloud-based architecture showing components and relationships between SAP NetWeaver BPM, Activiti, SVaaS-enabled components, and external services like U. of Genova and SAP Internal.]
Demo: Business Process Modeling
Demo: Business Process Level Reasoning
Demo: Implementation Level Reasoning

```java
public void execute(DelegateExecution ex) throws Exception {
    String lastname = (String) ex.getVariable("user_lastname");
    String firstname = (String) ex.getVariable("user_firstname");
    String email = (String) ex.getVariable("user_email");
    String reason = (String) ex.getVariable("travel_business_reason");
    String destination = (String) ex.getVariable("travel_destination");
    String duration = (String) ex.getVariable("travel_duration");

    // Code for accessing the web service
    QName SERVICE_NAME = new QName("http://travel.corp/", "TravelService");
    URL WSDLURL = new URL("http://travel.corp/TravelService/Service.asmx?WSDL");

    Service travelService = new Service(WSDLURL, SERVICE_NAME);
    ServiceSoap port = travelService.getServiceSoap();

    // send order to the service
    port.orderTravelAs
}
```

Read access to process variable "travel_business_reason" in line 26 violates the need to know principle of the process level task "Contact Travel Service Company".

Thank you!

