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 analyst. 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.
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

Demo: Business Process Modeling
Bibliography


