Integrated Model-driven Security: From Business Processes to Software Services

Bernhard Hoisl and Mark Strembeck

Competence Centers for Excellent Technologies
www.ffg.at/comet

Problem & Motivation

- **Specification and enforcement of process-level security properties**
- **Main problems:**
  - no native language constructs to model security features in current modeling languages
  - process modeling language different from system modeling language → mapping problem

Systematic Approach

- **CIM: Generic metamodels for process-related security properties**
- **PIM: Domain-specific modeling languages (DSMLs) for process-related security properties**
- **PSM: Enforcement of DSML specifications in software systems**
- **Transformations: CIM-to-PIM mapping (model-to-model) and PIM-to-PSM mapping (model-to-text)**

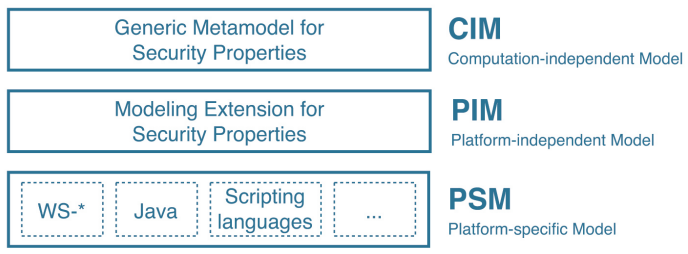

Figure 1: The approach supports all MDD layers

...
Definition 3.2: $\forall t_2 \in dme(t_1), pi \in P_I: \forall t_x \in ti(t_2, pi), t_y \in ti(t_1, pi): es(t_x) \cap es(t_y) = \emptyset$
Definition 3.3: $\forall t_2 \in rb(t_1), pi \in P_I: \forall t_x \in ti(t_2, pi), t_y \in ti(t_1, pi): er(t_x) = er(t_y)$
Definition 3.4: $\forall t_2 \in sb(t_1), pi \in P_I: \forall t_x \in ti(t_2, pi), t_y \in ti(t_1, pi): es(t_x) = es(t_y)$
...

Figure 2: Formal and generic definitions (CIM level)

Example: Secure Object Flows

- **CIM: Generic definition for data confidentiality and integrity**
- **PIM: Integration of secure object flows into the UML**
  - business-level: process view → security-extended UML activity models
  - service-level: SOA views → UML component structure, service activity, and secure invocation protocol
- **PSM: Web Services → WS-BPEL, WSDL, WS-SecurityPolicy**
- **Tool support for**
  - all modeling views (business processes, security properties, software services)
  - automatic model transformations
  - deployment of software artifacts in runtime engine

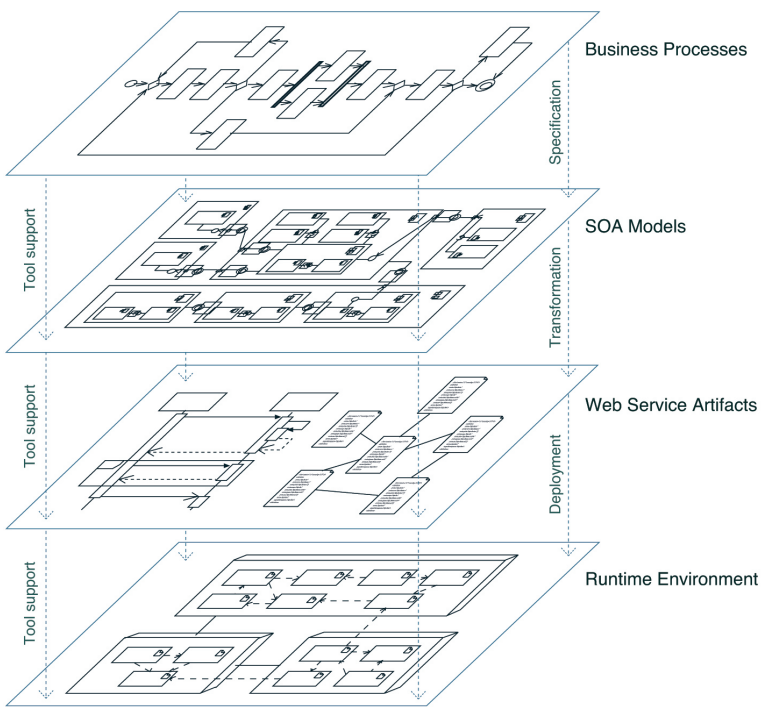

Figure 3: Integrated tool support for the definition and implementation of secure object flows

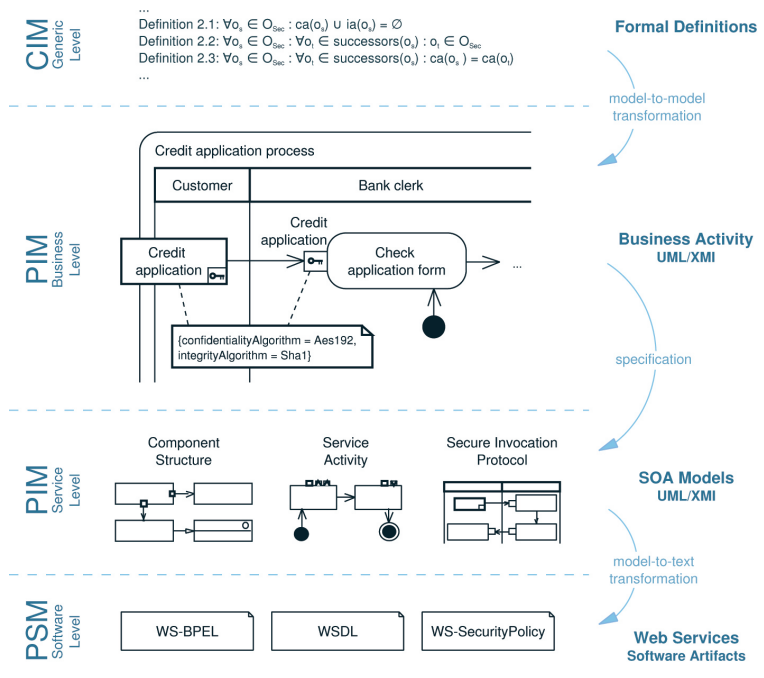

Figure 4: Different modeling levels, views, and transformations

References
B. Hoisl, S. Sobernig, and M. Strembeck: Modeling and Enforcing Secure Object Flows in Process-driven SOAs: An Integrated Model-driven Approach. In: Software and Systems Modeling (SoSyM), Springer, 2012, forthcoming
B. Hoisl, S. Sobernig, S. Schefer-Wenzl, M. Strembeck, A. Baumgrass: Design Decisions for UML and MOF based Domain-specific Language Models: Some Lessons Learned, In: Proc. of the 2nd Workshop on Process-based approaches for Model-Driven Engineering (PMDE), July 2012
B. Hoisl and M. Strembeck: A UML Extension for the Model-driven Specification of Audit Rules. In: Proc. of the 2nd International Workshop on Information Systems Security Engineering (WISSE), Springer LNBIP, Vol. 112, June 2012
B. Hoisl and S. Sobernig: Integrity and Confidentiality Annotations for Service Interfaces in SoaML Models. In: Proc. of the International Workshop on Security Aspects of Process-aware Information Systems (SAPAIS), IEEE CPS, August 2011
B. Hoisl and M. Strembeck: Modeling Support for Confidentiality and Integrity of Object Flows in Activity Models. In: Proc. of the 14th International Conference on Business Information Systems (BIS2011), Springer LNBIP, Vol. 87, June 2011
M. Strembeck and J. Mendling: Modeling Process-related RBAC Models with Extended UML Activity Models. In: Information and Software Technology (IST), Vol. 53, No. 5, May 2011

Das Kompetenzzentrum SBA Research wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMVIT, BMWFJ, das Land Wien gefördert. Das Programm COMET wird durch die FFG abgewickelt.