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

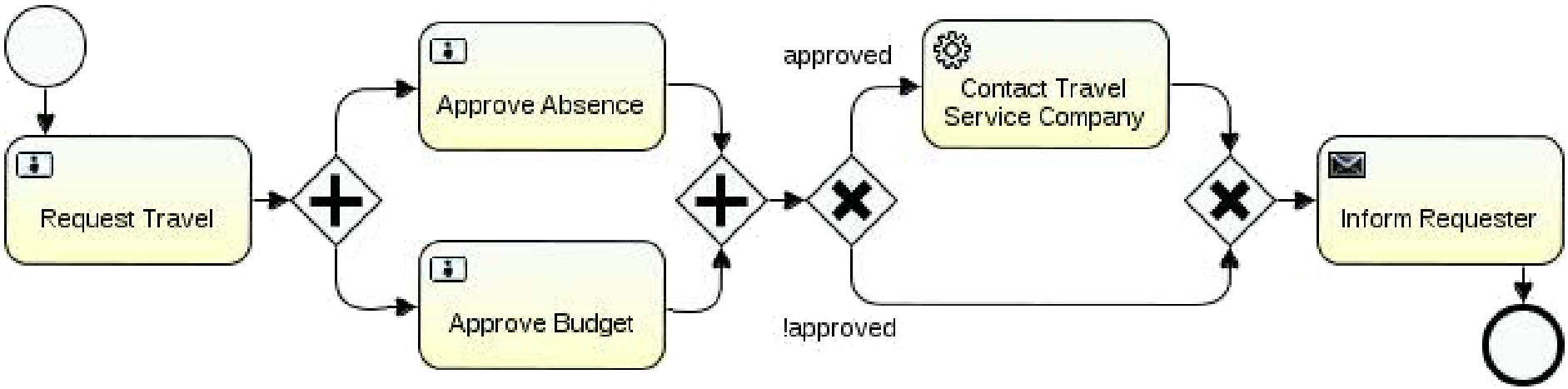
Dagstuhl Seminar 13211: “Automated Reasoning on Conceptual Schemas”
http://www.dagstuhl.de/13211

19.05.2013 – 24.05.2013

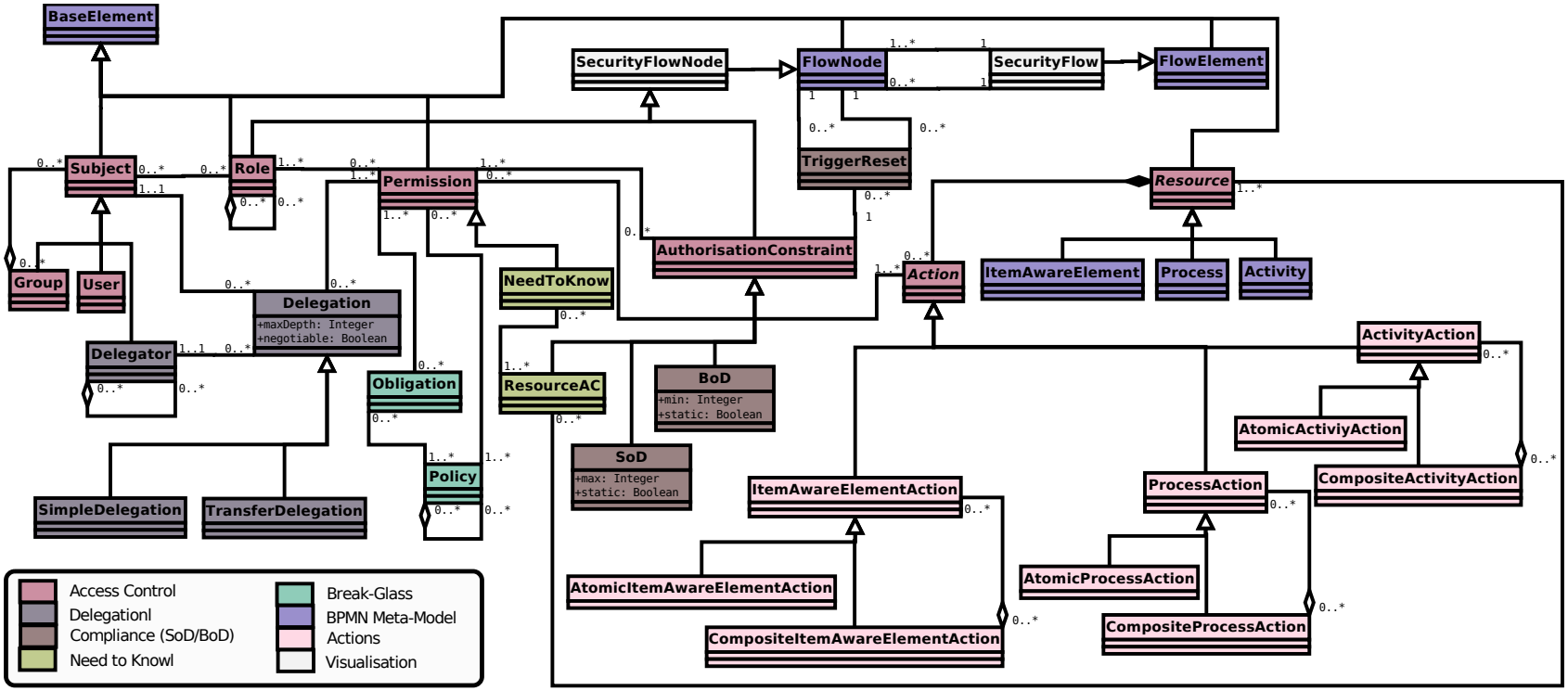
Abstract

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.

Business Process Modeling



SecureBPMN



- 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

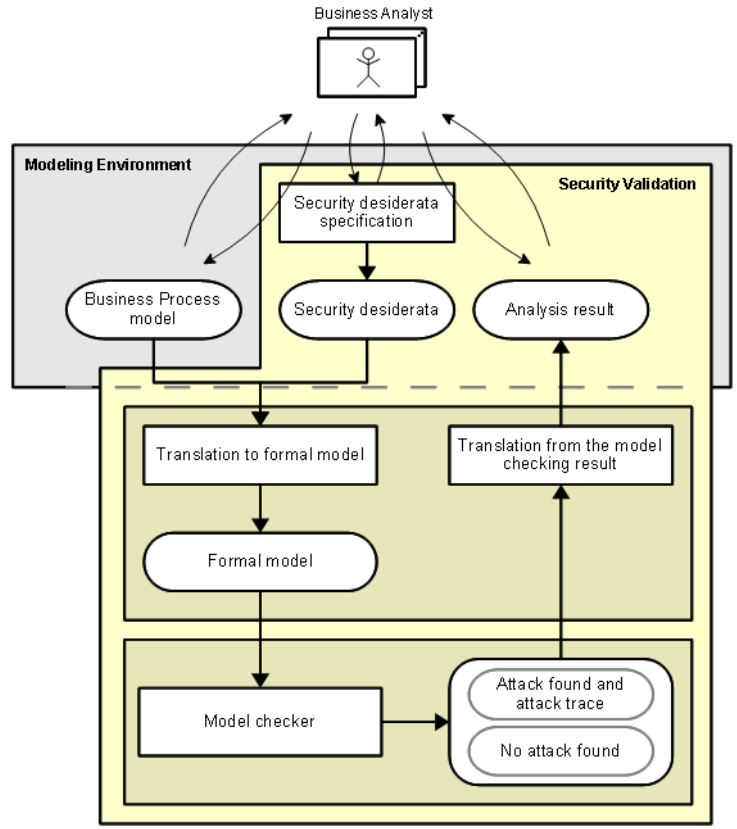
- Process level
  - consistency of security specifications
  - static vs. dynamic enforcement
  - . . .
- Implementation level
  - access control infrastructure
  - data flows (confidentiality)
  - . . .

How to Check

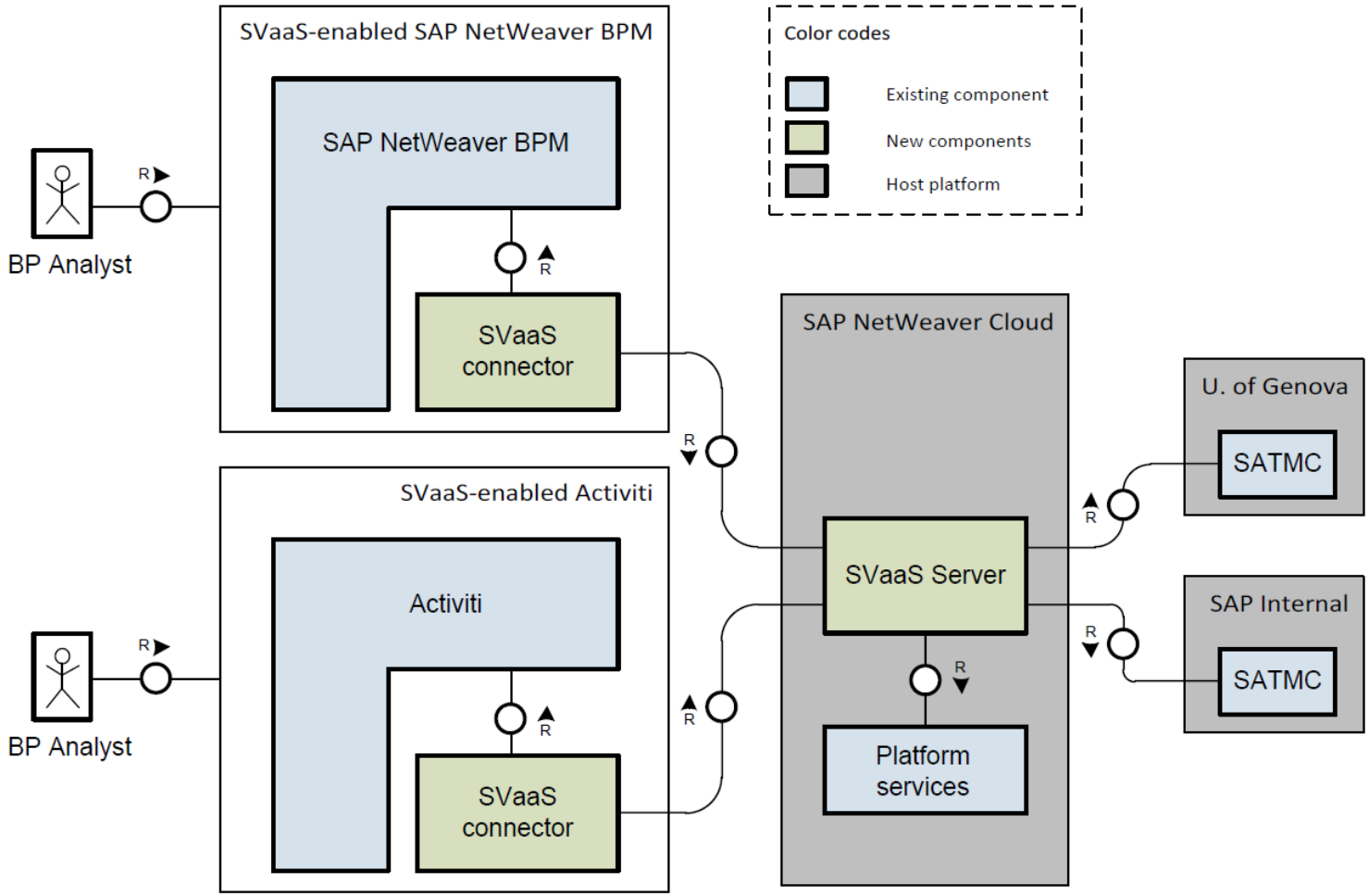
- Model checking
- Theorem proving (e.g., SMT)
- Static code analysis

Security Validation of Business Process

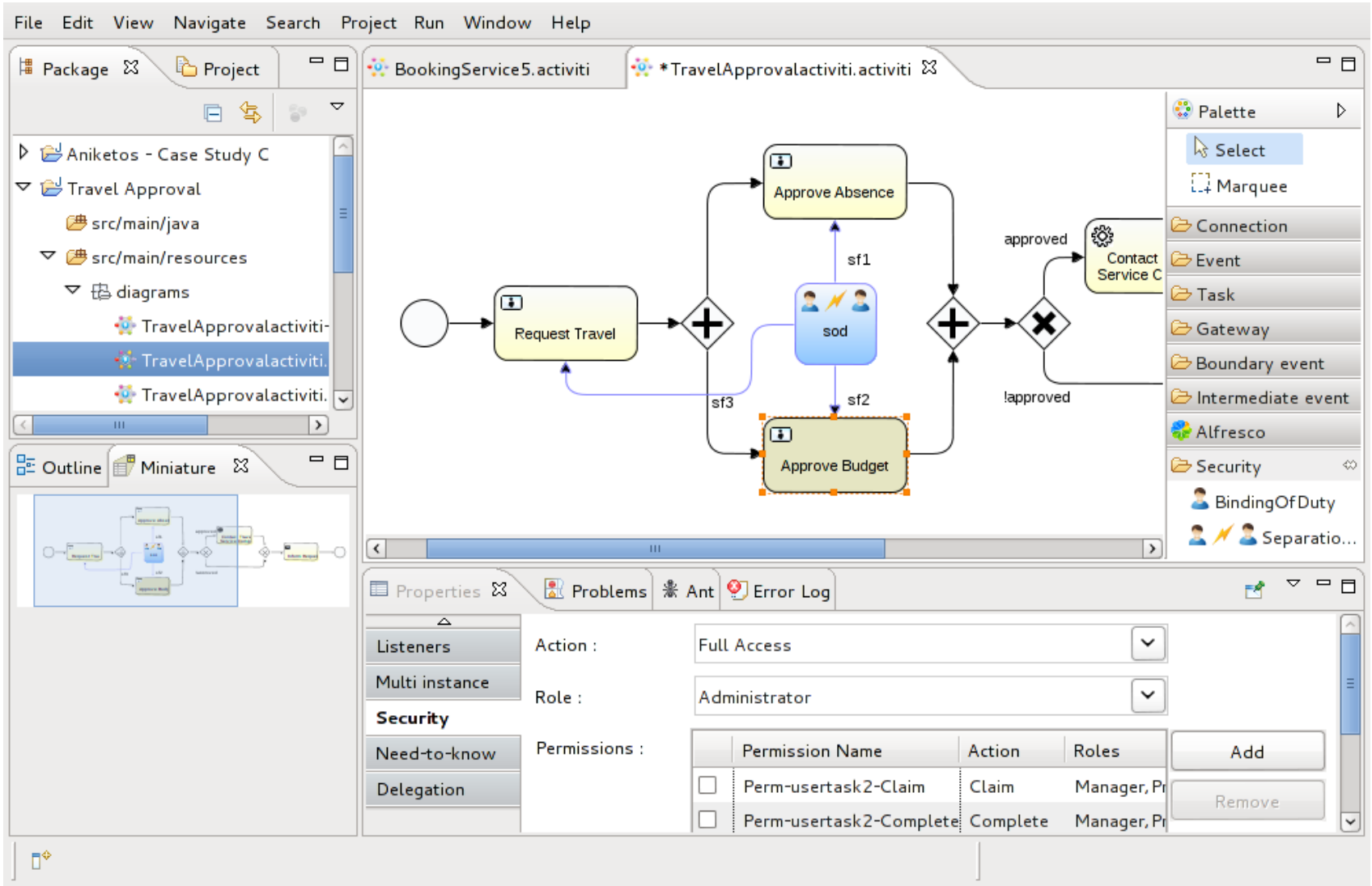
- Express security requirements
- Detect vulnerabilities at design time
- Highlight execution paths leading to a security violation so to provide guidelines in solving the problem
- Mitigate the deployment of non-compliant business processes



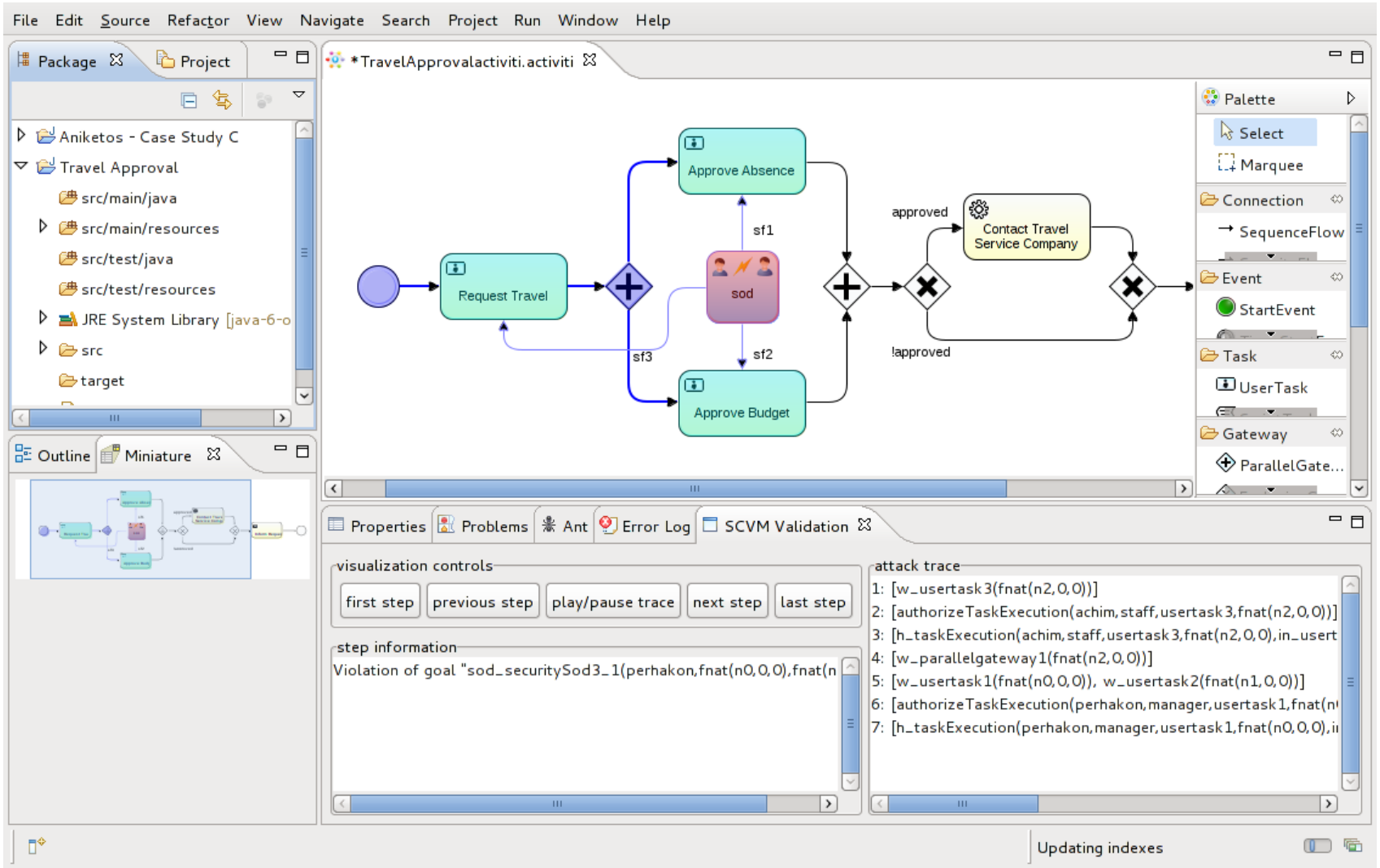
A Cloud-based Architecture



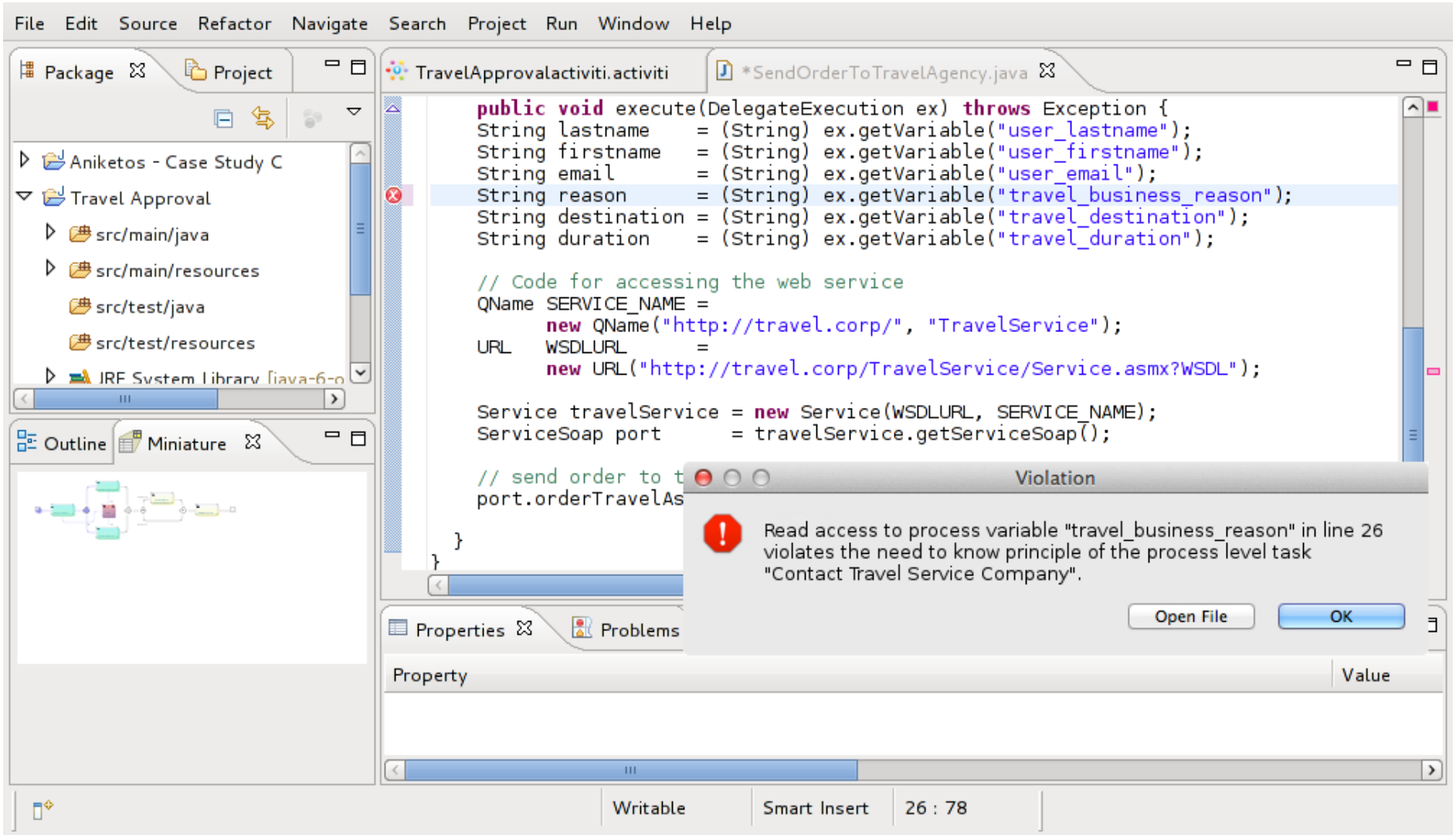
Demo: Business Process Modeling



Demo: Business Process Level Reasoning



Demo: Implementation Level Reasoning



Thank you!

Bibliography

Achim D. Brucker and Isabelle Hang. Secure and compliant implementation of business process-driven systems. In Marcello La Rosa and Pnina Soffer, editors, *Joint Workshop on Security in Business Processes (SBP)*, volume 132 of *Lecture Notes in Business Information Processing (LNBIP)*, pages 662–674. Springer-Verlag, 2012.

`http://www.brucker.ch/bibliography/abstract/brucker.ea-secure-2012`.

Achim D. Brucker, Isabelle Hang, Gero Lückemeyer, and Raj Ruparel. SecureBPMN: Modeling and enforcing access control requirements in business processes. In *ACM symposium on access control models and technologies (SACMAT)*, pages 123–126. ACM Press, 2012.

`http://www.brucker.ch/bibliography/abstract/brucker.ea-securebpmn-2012`.

Luca Compagna, Pierre Guilleminot, and Achim D. Brucker. Business process compliance via security validation as a service. In Manuel Oriol and John Penix, editors, *Testing Tools Track of International Conference on Software Testing, Verification, and Validation (Tools@ICST)*. IEEE Computer Society, 2013.

`http://www.brucker.ch/bibliography/abstract/compagna.ea-bp-compliance-2013`.

© 2013 SAP AG. All rights reserved