

Reasoning over Secure Business Processes

Achim D. Brucker
achim.brucker@sap.com

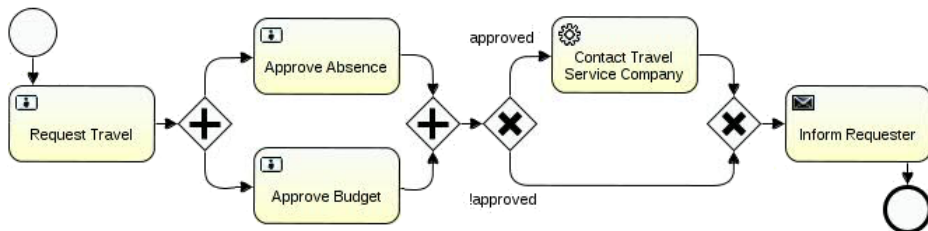
joint work with Luca Compagna, Pierre Guillemot, and Isabelle Hang

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



Business Process Modeling

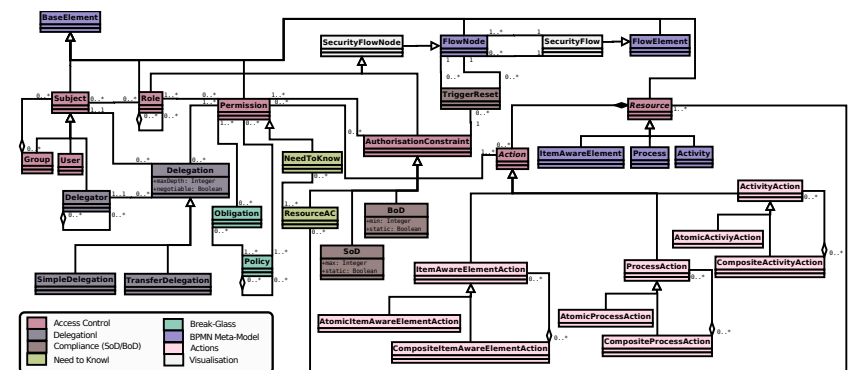


Abstract

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.

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

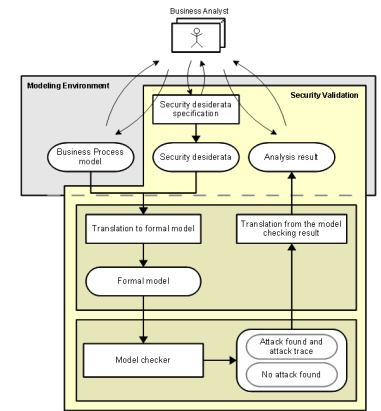
- Process level
 - consistency of security specifications
 - static vs. dynamic enforcement
 - ...
- Implementation level
 - access control infrastructure
 - data flows (confidentiality)
 - ...

How to Check

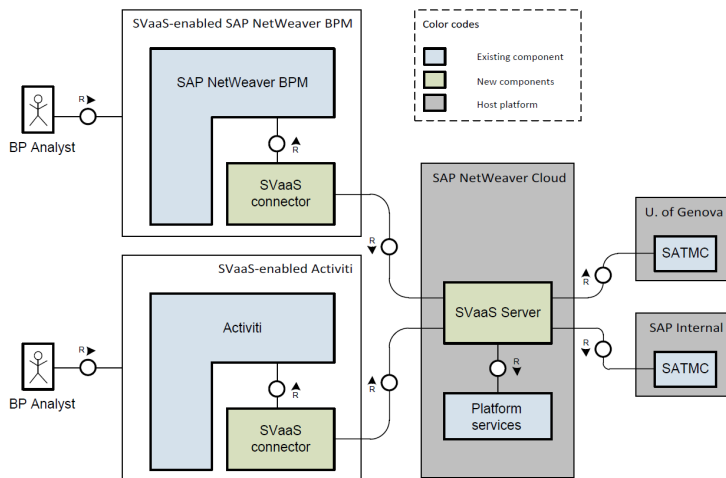
- Model checking
- Theorem proving (e.g., SMT)
- Static code analysis

Security Validation of Business Process

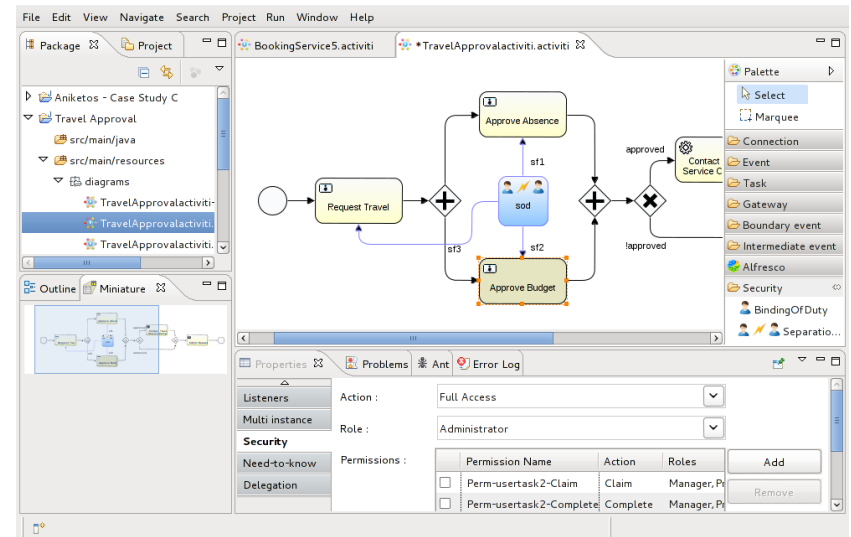
- Express security requirements
- Detect vulnerabilities at design time
- Highlight execution paths leading to a security violation so to provide guidelines in solving the problem
- Mitigate the deployment of non-compliant business processes



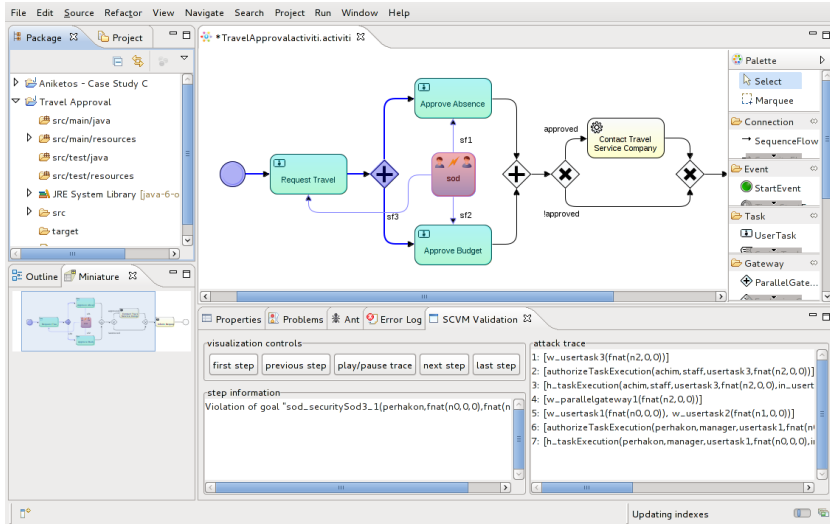
A Cloud-based Architecture



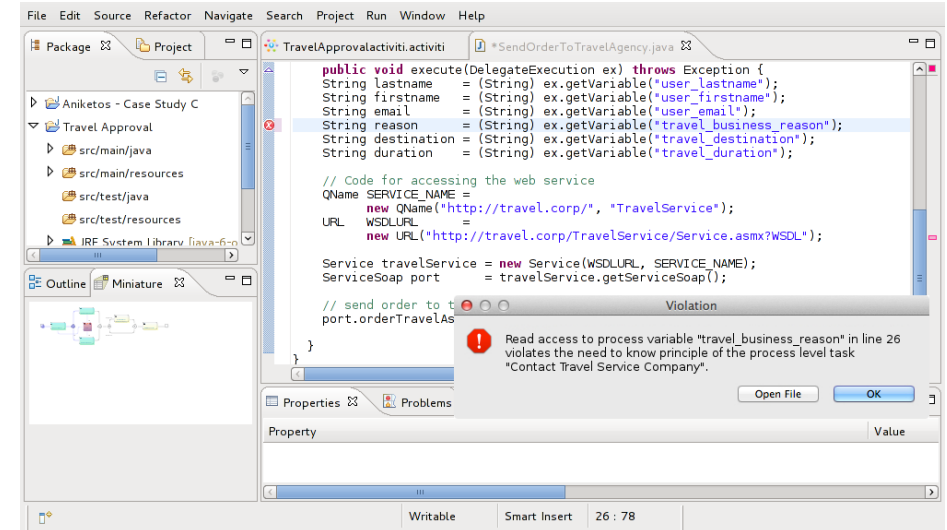
Demo: Business Process Modeling



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-securebpnm-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.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice. Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation. IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. Oracle is a registered trademark of Oracle Corporation. UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group. Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc. HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology. Java is a registered trademark of Sun Microsystems, Inc. JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape. SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company. Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary. The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG. This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice. SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence. The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.