

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>

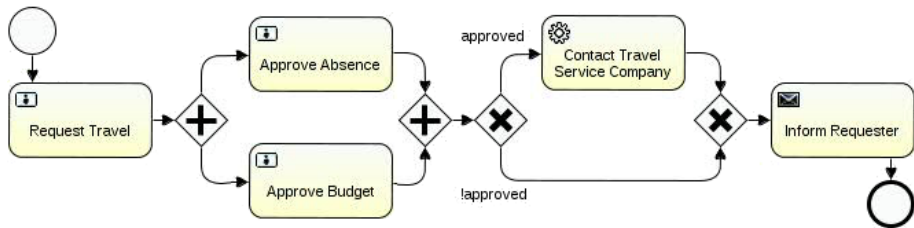
19.05.2013 – 24.05.2013

Abstract

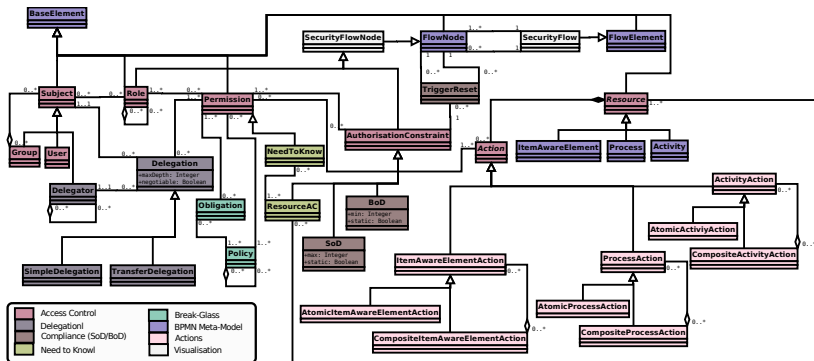
Modern enterprise systems are often process-based, i.e., they allow for the direct execution of business processes that are specified in a high-level language such as BPMN.

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

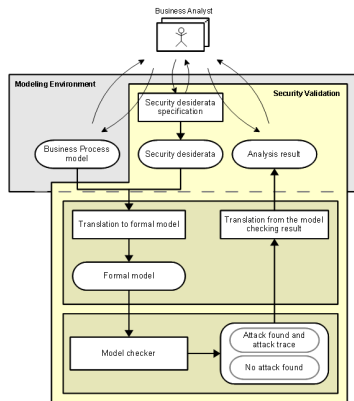
- Process level
 - consistency of security specifications
 - static vs. dynamic enforcement
 - ...
- Implementation level
 - access control infrastructure
 - data flows (confidentiality)
 - ...

How to Check

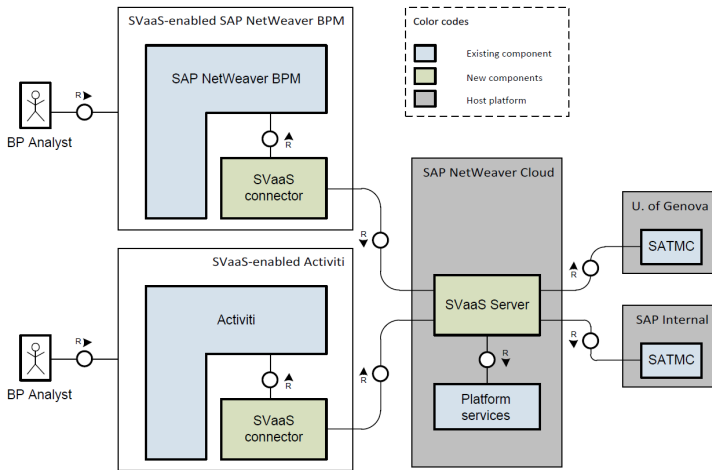
- Model checking
- Theorem proving (e.g., SMT)
- Static code analysis

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

The screenshot displays the SAP Business Process Modeler (BPM) interface. The main workspace shows a process diagram for 'Travel Approval' with the following elements:

- Start Event:** A circle leading to a 'Request Travel' task.
- Split Gateway:** A diamond with a plus sign (+) that branches the flow into two parallel paths.
- Parallel Tasks:** 'Approve Absence' (yellow) and 'Approve Budget' (green). Both are connected to a central 'sod' (Separation of Duties) task (blue).
- Flow Labels:** 'sf1' connects 'Approve Absence' to 'sod', and 'sf2' connects 'Approve Budget' to 'sod'. 'sf3' connects 'sod' back to 'Request Travel'.
- Join Gateway:** A diamond with a plus sign (+) that merges the flows from 'Approve Absence' and 'Approve Budget'.
- Exclusive Gateway:** A diamond with an 'X' that branches the flow into two paths: 'approved' leading to a 'Contact Service C' task, and 'lapproved' leading to another task.

The left sidebar shows the project structure for 'Aniketos - Case Study C' > 'Travel Approval' > 'src/main/resources' > 'diagrams'. The 'TravelApprovalactiviti...' diagram is selected.

The right sidebar is the 'Palette' containing various BPM elements like Connection, Event, Task, Gateway, Boundary event, Intermediate event, Alfresco, Security, BindingOfDuty, and Separatio...

The bottom panel shows the 'Properties' view for the selected element, with the following configuration:

- Listeners:** Action: Full Access
- Multi instance:** (empty)
- Security:** Role: Administrator
- Need-to-know:** (empty)
- Delegation:** (empty)

The 'Permissions' table is also visible:

Permission Name	Action	Roles	Add
<input type="checkbox"/> Perm-usertask2-Claim	Claim	Manager, Pr	
<input type="checkbox"/> Perm-usertask2-Complete	Complete	Manager, Pr	

Demo: Business Process Level Reasoning

The screenshot displays the SAP Business Process Manager (BPM) interface. The main window shows a process diagram for 'TravelApprovalactiviti.activiti'. The process starts with a 'Request Travel' task, followed by a parallel gateway. This gateway splits into three paths: 'Approve Absence', 'sod' (Security Object Definition), and 'Approve Budget'. The 'sod' task is connected to 'sf1' and 'sf2' (Service Flows). The 'Approve Absence' and 'Approve Budget' tasks merge at another parallel gateway. This gateway leads to a decision gateway with two outgoing paths: 'approved' leading to 'Contact Travel Service Company' and 'approved' leading to another decision gateway. The 'Contact Travel Service Company' task also leads to a decision gateway. The process ends with a final decision gateway.

The bottom panel shows the 'attack trace' log, which contains the following entries:

```
attack trace
1: [w_usertask 3(fnat(n2, 0, 0))]
2: [authorizeTaskExecution(achim, staff, usertask 3, fnat(n2, 0, 0))]
3: [h_taskExecution(achim, staff, usertask 3, fnat(n2, 0, 0), in_usertask 3, fnat(n2, 0, 0))]
4: [w_parallelgateway 1(fnat(n2, 0, 0))]
5: [w_usertask 1(fnat(n0, 0, 0)), w_usertask 2(fnat(n1, 0, 0))]
6: [authorizeTaskExecution(perhakon, manager, usertask 1, fnat(n1, 0, 0))]
7: [h_taskExecution(perhakon, manager, usertask 1, fnat(n0, 0, 0), in_usertask 1, fnat(n0, 0, 0))]
```

The 'step information' section shows a violation of goal 'sod_securitySod3_1(perhakon,fnat(n0,0,0),fnat(n1,0,0))'.

Demo: Implementation Level Reasoning

The screenshot shows an IDE window with the following components:

- Menu Bar:** File, Edit, Source, Refactor, Navigate, Search, Project, Run, Window, Help
- Package Explorer:** Shows a project structure for "Aniketos - Case Study C" with sub-packages: "Travel Approval", "src/main/java", "src/main/resources", "src/test/java", "src/test/resources", and "JRE System Library [java-6-0]".
- Code Editor:** Displays the file `*SendOrderToTravelAgency.java`. The code includes:

```
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 t
    port.orderTravelAs
}
}
```
- Violation Dialog:** A modal dialog titled "Violation" with a red exclamation mark icon. The message reads: "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'." Buttons for "Open File" and "OK" are visible.
- Properties and Problems:** The "Properties" tab is active, showing a table with "Property" and "Value" columns. The "Problems" tab is also visible.
- Status Bar:** Shows "Writable", "Smart Insert", and "26 : 78".

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 Guillemot, 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:](http://www.brucker.ch/bibliography/abstract/compagna.ea-bp-compliance-2013)

[//www.brucker.ch/bibliography/abstract/compagna.ea-bp-compliance-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.