

Secure and Compliant Implementation of Business Process-driven Systems

Achim D. Brucker Isabelle Hang
{achim.brucker, isabelle.hang}@sap.com

SAP AG, SAP Research, Security & Trust
Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany



SAP RESEARCH

Our Goal:

End-to-End Secure and Compliant Processes

“

Extending workflow management systems with means for specifying, analyzing, and enforcing security and compliance properties across all (system) layers.

Today:

- Static enforcement of security and compliance requirements
 - Applying static (program) analysis to service/task implementations
 - Prototype based on Activiti BPM Platform

Observations:

- There are many approaches for modeling secure business processes
- Runtime enforcement (monitoring) is expensive
- Static program analysis works well for ensuring application security

Agenda

1 Motivation

2 Static (Program) Analysis for Security and Compliance PBMSs

3 Conclusion

Secure Business Processes

A Simple Example: A Travel Approval Process

The screenshot displays the SAP Business Process Manager (BPM) interface for a travel approval process. The main canvas shows a flowchart with the following elements:

- Request Travel** (Task): The starting point of the process.
- SoD** (Separation of Duties) constraints: Three blue boxes with lightning bolt icons are placed around the process flow.
- Approval** (Task): A yellow box that branches into two parallel paths.
- Approve Duration** (Task): A yellow box in the top parallel path.
- Approve Budget** (Task): A yellow box in the bottom parallel path.
- Send Result** (Task): A yellow box that receives input from both parallel paths and leads to the end of the process.

The **Properties** panel at the bottom shows the configuration for the selected task:

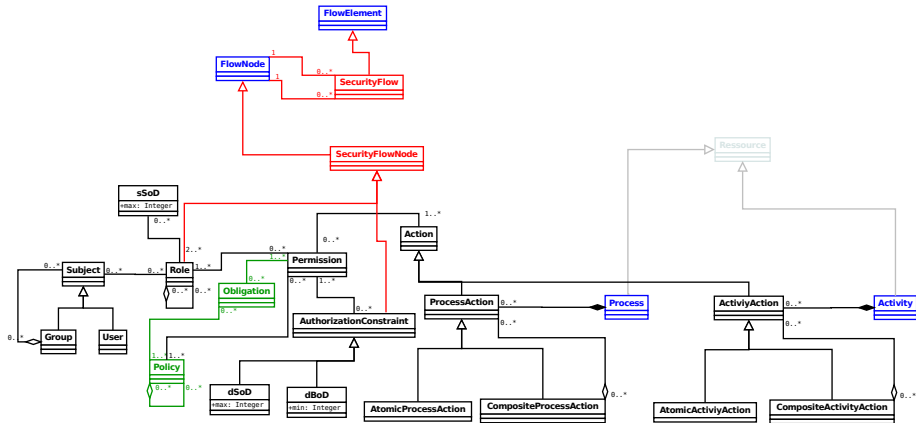
- Action**: Claim
- Role**: Clerk
- Permissions**: A table listing permissions for the role.

Permission Name	Action	Roles
<input type="checkbox"/> Perm-usertask3-Full Access	Full Access	Manager

The **Palette** on the right lists various BPM elements such as Select, Marquee, Connection, Event, Task, Gateway, and Security.

The SecureBPMN Meta-Model

A Meta-model-based Extension of BPMN

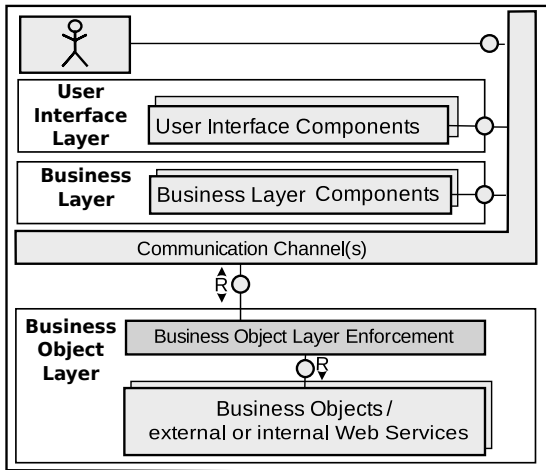


- Hierarchical RBAC
- Fine-grained SoD/BoD
- Need to know
- Break-glass support
- Delegation
- ...

Modern Business Process Execution

Cloud- or SoA-based Business Process Execution

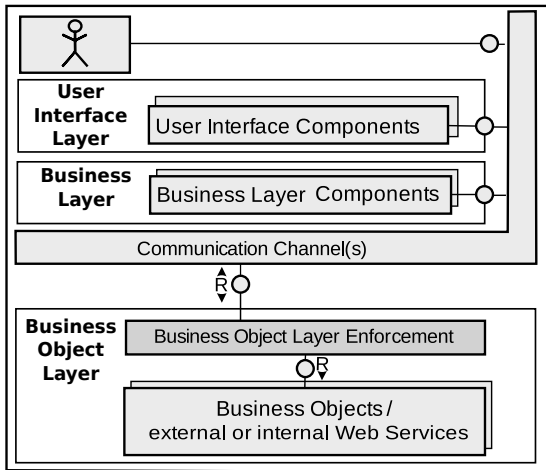
- PBMSs integrate many (technical) layers
- Security needs to be checked on all layers
- Layers may be operated by different parties
- Executable process models are not enough



Modern Business Process Execution

Cloud- or SoA-based Business Process Execution

- PBMSs integrate many (technical) layers
- Security needs to be checked on all layers
- Layers may be operated by different parties
- Executable process models are not enough
 - Implementation of service tasks
 - User interfaces for human tasks



Has Sony been Hacked this Week?

<http://hassonybeenhackedthisweek.com/>

Time-line of the Sony Hack(s) (excerpt):

- 2011-04-20 Sony PSN goes down
- 2011-05-21 Sony BMG Greece: data of 8300 users leaked (SQL Injection)
- 2011-05-23 Sony Japanese database leaked (SQL Injection)
- 2011-05-24 Sony Canada: roughly 2,000 leaked (SQL Injection)
- 2011-06-05 Sony Pictures Russia (SQL Injection)
- 2011-06-06 Sony Portugal (SQL injection, iFrame injection and XSS)
- 2011-06-20 20th breach within 2 months
177k email addresses were grabbed (SQL injection)

(<http://hassonybeenhackedthisweek.com/history>)

A Bluffers Guide to SQL Injection

- **Assume an SQL Statement for**

selecting all users with a specific "user name" from a table "user"

A Bluffers Guide to SQL Injection

- **Assume an SQL Statement for**

```
statement="SELECT * FROM 'users' WHERE 'name' = '" + userName + "';"
```

A Bluffers Guide to SQL Injection

- **Assume an SQL Statement for**

```
statement="SELECT * FROM 'users' WHERE 'name' = '" + userName + "';"
```

- **What happens if we choose the following (weird) userName:**

```
userName = "' or '1'='1"
```

A Bluffers Guide to SQL Injection

- **Assume an SQL Statement for**

```
statement="SELECT * FROM 'users' WHERE 'name' = '" + userName + "';"
```

- **What happens if we choose the following (weird) userName:**

```
userName = "' or '1'='1"
```

- **Resulting in the following statement:**

```
statement = "SELECT * FROM 'users' WHERE 'name' = '' or '1'='1';"
```

A Bluffers Guide to SQL Injection

- **Assume an SQL Statement for**

```
statement="SELECT * FROM 'users' WHERE 'name' = '" + userName + "';"
```

- **What happens if we choose the following (weird) userName:**

```
userName = "' or '1'='1"
```

- **Resulting in the following statement:**

```
statement = "SELECT * FROM 'users' WHERE 'name' = '' or '1'='1';"
```

- **Which is equivalent to**

```
statement = "SELECT * FROM 'users';"
```

selecting the information of **all users** stored in the table "users"!

Static Program Analysis

Static Application Security Testing



Users of Applications should not be able to influence SQL statements!

```
void selectUser(HttpServletRequest req, HttpServletResponse resp, bool c)
    throws IOException {
    String userName    = req.getParameter("fName");
    String statement = "SELECT * FROM 'users' WHERE 'name' = '"
        + userName + "'";
    SQL.exec(statement);
}
```

- We have a method that analyzes applications without running them
 - detects implementation level security problems
 - use of unwanted commands or API calls
 - unwanted data flows and control flows
- Can we apply static program analysis to PBMSs
 - ensure security of service task implementations
 - statically check security and compliance requirements

Agenda

- 1 Motivation
- 2 Static (Program) Analysis for Security and Compliance PBMSs
- 3 Conclusion

Applying Static (Program Analysis) to PBMSs

“

Infer requirements on the **implementation level** from **process level specification** of security and compliance requirements and use static analysis to check them

Implementation (examples):

- Source code of **service tasks**
- Source code of the user interfaces of **human tasks**
- System configurations

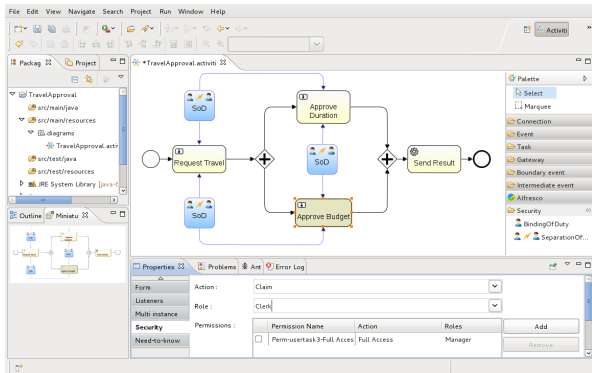
Static checks (examples):

- **Access control**: check presence of access control checks (e. g., PEPs)
- **Separation of Duty**: check control flow
- **Need to Know**: check access to process variables or messages and derived data (data flow as well as control flow)

Secure Business Processes

A Simple Example: A Travel Approval Process

- Access Control
- Separation of Duty
- *Need to Know*



Need to Know (User Interface)

Approve Duration

```
<userTask id="Approve Duration">
  <extensionElements>
    <activiti:formProperty id="user_lastname" writable="false"/>
    <activiti:formProperty id="user_firstname" writeable="false"/>
    <activiti:formProperty id="travel_destination" writeable="false"/>
    <activiti:formProperty id="travel_duration" writeable="false"/>
    <activiti:formProperty id="travel_budget" writeable="false"/>
  </extensionElements>
</userTask>
```

There are two violations of a strict need to know principle

- Read access to **travel_destination**
- Read access to **travel_budget**

The access to **travel_budget** may violate the separation of duty

Backdoors in Service Implementations

SendResult

```
public class SendResult implements JavaDelegate {
    public void execute(DelegateExecution execution) throws Exception {
        String lastname    = (String) execution.getVariable("user_lastname");
        String firstname    = (String) execution.getVariable("user_firstname");
        ...

        if (firstname.equals("eve"))
            execution.setVariable("travel_budget",
                (new Integer(execution.getVariable("travel_budget")*2)).toString());

        sendEmail(firstname, lastname, email, destination, duration);
    }
}
```

- **Here:** writing to `travel_budget` violates the need to know principle
- **In general:** an interesting research topic

Agenda

- 1 Motivation
- 2 Static (Program) Analysis for Security and Compliance PBMSs
- 3 Conclusion**

Conclusion

“

Static analysis complements (**not** replaces) run-time methods or system audits.

- Multi-layered Process Security:
 - Runtime-checks (monitoring) on all layers
 - Static check (source code, configuration, ...)
 - Post-hoc audits
- Cost reduction and efficiency improvements:
 - Reduction of required runtime resource (time, memory, ...)
 - Reduction of resources required for (compliance) audits
- Many open questions:
 - What can static analysis offer on the process level
 - How to choose the right balance (for a specific use case)
 - How to express all properties on the process level
 - ...

Thank you!



Related Publications



Achim D. Brucker and Isabelle Hang.

Secure and compliant implementation of business process-driven systems.

In *Joint Workshop on Security in Business Processes (sbp!)*, Lecture Notes in Business Information Processing (LNBIP). Springer, 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 SACMAT*, pages 123–126. ACM Press, 2012.

ISBN 978-1-4503-1295-0.

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

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+, POWERS, 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.