BPM and Cloud Integration
A New Driver for Research in Security in Business Processes

Achim D. Brucker
achim.brucker@sap.com

SAP AG, P&I ACES, Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany

Guest Lecture: Konzepte und Anwendung von Workflowsystemen
Karlsruhe Institute of Technology (KIT)
13.02.2014
Abstract

Enterprise systems in general and process aware systems in particular are storing and processing the most critical assets of a company. To protect these assets, such systems need to implement a multitude of security properties. Moreover, such systems need often to comply to various compliance regulations.

In this talk, we briefly discuss challenges of implementing large-scale systems based on workflow-management in general and, in particular, the in the context of cloud based systems. We will put a particular focus on security requirements and discuss the gap between the ideal world of process-aware information systems and the real world. We conclude our presentation by discussing several research challenges in the area of verifiable secure process aware information systems.
Agenda

1. SAP and SAP P&I ACES
2. Process-aware Information Systems
4. Research Directions and Challenges
5. Conclusion
1 SAP and SAP P&I ACES

2 Process-aware Information Systems
   - The Ideal World
   - The Real World
   - Cloud Integration
   - System Complexity and Adoption Rate

3 Security, Trust, and Compliance of Business Processes

4 Research Directions and Challenges

5 Conclusion
Die SAP AG

• Leader in Business Software
• Vendor process-aware systems
• More than 25 industries
• 63% of the world’s transaction revenue touches an SAP system
• 64,422 employees worldwide
• Headquarters:
  Walldorf (and St. Leon-Rot)
• Location in Karlsruhe:
  ca. 500m from here
SAP P&I ACES: Mission

**Mission**
- Orchestrating the architecture definition and communicating the results consistently
- Building the best educated development organization in- and outside the company
- Making Security a key differentiator for choosing SAP

**Goals**
- **Architecture**: Lead the way we jointly create and manage the architecture of our products
- **Communication**: Roll-out this architecture consistently to our field colleagues, customers and partners.
- **Education**: Drive education for developers internally & externally - ensure that it is fun to learn SAP, renew education concepts and technology.
- **Security**: Drive Product Security, transform it to become a differentiator for SAP.
My Background

• Senior Researcher at SAP AG
  • Product Security Research
  • Code Analysis

• Background:
  Security, Formal Methods, Software Engineering

• Current work areas:
  • Security in business processes
  • Static code analysis (u.a. für JavaScript)
  • Security Testing
Agenda

1. SAP and SAP P&I ACES
2. Process-aware Information Systems
4. Research Directions and Challenges
5. Conclusion
Ideal World: Modeling
Real World: Modeling

Process Models:
- BPMN/BPEL
- Configurable transactions
- Custom Coding
- Legacy Systems
- External services

Security:
- Each system (OS, DB, IS)
  - own security infrastructure
  - own logging infrastructure
- Management solutions try to bridge this gap
Real World: Deployment and Execution

**Backend:**
- AS Java, AS ABAP
- Business Process Engine
- Legacy Systems
- External services
- Sensors and product lines

**Frontend:**
- Desktop clients
- Web-based clients
- Mobile clients
- Client side compositions (e.g., mash-ups)
Customers have complex on-premise landscapes.

As customers adopt cloud solutions, hybrid landscapes will become a norm.

Integration across the boundaries of cloud and on-premise is a must to prevent application silos.

As companies adopt cloud, real-time end-to-end business process integration is critical.
How the Future Might Look Like

Cloud Solutions

Cloud + CRM
Cloud for Customer

Two-tier CRM
Cloud for Customer
Subsidiaries
Pre-Built and Maintained Integrations (iFlows)

Cloud + ERP
Cloud for Customer

Cloud + 3rd Party
Cloud for Customer

On-premise Solutions

SAP CRM
SAP ERP

SAP CRM
SAP ERP

SAP ERP
3rd Party System
Customer Example (1/2)

- Large manufacturing company with SAP ERP, multiple legacy HR and other financial applications worldwide
- Migration from legacy HR system
- >120 third-party interfaces – Integration of third-party cloud solutions to Employee Central (EC) and EC Payroll
- 100% of SAP-to-SAP integrations and 30% of all integrations covered by prepackaged integration flows (iFlows)
Industrial manufacturer with multiple subsidiaries on different SAP ERP clients as well as third-party ERP systems

- Rapid implementation with small IT team
- Delivered improved usability for field sales and collaboration between field sales and back office
- Integration of accounts, materials, sales quotes and sales orders
Evolution of Source Code

- Increase in
  - code size
  - code complexity
  - number of products
  - product versions
Support Lifecycle (Maintenance)
## Support Lifecycle (Maintenance)

### Example (Maintenance Cycles)

<table>
<thead>
<tr>
<th>Produkt</th>
<th>Release</th>
<th>EOL</th>
<th>ext. EOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>2001</td>
<td>2009</td>
<td>2014</td>
</tr>
<tr>
<td>Windows 8</td>
<td>2012</td>
<td>2018</td>
<td>2023</td>
</tr>
<tr>
<td>Red Hat Ent. Linux</td>
<td>2012</td>
<td>2020</td>
<td>2023</td>
</tr>
<tr>
<td>SAP ERP</td>
<td>2004</td>
<td>2020</td>
<td>&gt; 2024</td>
</tr>
</tbody>
</table>

Maintenance fees: typical 20% of the original price
## Customer Requirements

<table>
<thead>
<tr>
<th>LOB*</th>
<th>IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single source of truth and master data synchronization</td>
<td>Data security and compliance</td>
</tr>
<tr>
<td>Real-time business process integration</td>
<td>Support for complex landscapes</td>
</tr>
<tr>
<td>Integrated user experience</td>
<td>Choice of integration technology</td>
</tr>
<tr>
<td>Rapid deployment</td>
<td>End-to-end monitoring and support</td>
</tr>
</tbody>
</table>

*Line of business*
Agenda

1. SAP and SAP P&I ACES
2. Process-aware Information Systems
4. Research Directions and Challenges
5. Conclusion
Security in Business Processes: An Example

[Diagram showing a business process flowchart with nodes labeled "Request Travel", "Approve Absence", "Approve Budget", "Contact Travel Service Company", and "Inform Requester". The flowchart outlines the steps and decision points in the process.]
Access Control

Goal:
- Control access to Tasks, Resources (Data), ...

The core:
- Usually:
  Users, Roles, Access Rights, ...
- In special cases:
  Data labeling

On top:
- Separation of Duty
- Binding of Duty
- Delegation
Protecting Data (and Goods)

Goal:
• Ensure
  • confidentiality
  • integrity (safety)
of data (and goods)

The core:
• Need-to-Know
• Fingerprints
• Encryption
• Sensors
Many regulated markets
- Basel II/III, SoX, PCI
- HIPAA

Many customer-specific regulations
- Own governance to mitigate risks
- Own business code of conduct
- Fraud detection/prevention
- Non-observability

Customers are individually audited
- No “one certificate fits all” solution

Security should not hinder business
Agenda

1. SAP and SAP P&I ACES
2. Process-aware Information Systems
4. Research Directions and Challenges
5. Conclusion
Our Research Over the Last Decade

Access Control for Processes
- RBAC-like models
- Delegation models
- Break-(the)-glass models

Model-driven Security
- Modeling of Security
- Generation of implementation, configuration
- Monitoring based on models

Process-level Verification
- Compliance to security spec.
- Consistency of security configurations

Implementation-level Verification
- Compliance of implementation to process level security req.
Research Challenges

Adaptability:
- How to extend systems safely
- Integration of legacy systems

Auditability:
- Coherent audit across providers/systems
- Reduction of audit costs

Cloud (SaaS):
- How to manage decentralized systems
- How to capture behavior of the composition
- Who is the attacker

Process level vs. technical levels:
- Security is more than CIA
- Ensuring secure implementation
Agenda

1. SAP and SAP P&I ACES
2. Process-aware Information Systems
4. Research Directions and Challenges
5. Conclusion
The most interesting challenges are still ahead of us!

- Real systems are large and complex:
  - many programming languages or frameworks
  - many security technologies
  - highly distributed
  - implement business processes in many different ways
- Many research is done on the process level
- We now need to bring the
  - process level
  - implementation level
  
  closer together to provide end-to-end security
- Cloud solutions create new challenges:
  - data protection across different providers
  - new attacker models
Thank you!

Interested in an Internship/Thesis at SAP:

- achim.brucker@sap.com
- www.sap.com/jobs/ and search for location “Karlsruhe” or “student”
Wihem Arsac, Luca Compagna, Giancarlo Pellegrino, and Serena Elisa Ponta.
Security validation of business processes via model-checking.

Achim D. Brucker and Isabelle Hang.
Secure and compliant implementation of business process-driven systems.

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.
Luca Compagna, Pierre Guilleminot, and Achim D. Brucker.  
Business process compliance via security validation as a service.  

Christian Wolter, Andreas Schaad, and Christoph Meinel.  
Deriving XACML policies from business process models.  
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.