Security in the Context of Business Processes
Thoughts from a System Vendor’s Perspective

Achim D. Brucker
achim.brucker@sap.com

SAP AG, Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany
http://www.dagstuhl.de/13341
18.08.2013 – 23.08.2013
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 keynote, we present process-level security requirements as well as 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.
1. Security, Trust, and Compliance of Business Processes
2. Process-aware Information Systems
3. Research Directions and Challenges
4. Conclusion
Point of View

Overall:
- Vendor process-aware systems
- More than 25 industries
- 63% of the world’s transaction revenue touches an SAP system
- 64,422 employees worldwide

Personal Background:
- Researcher (SE, FM, Security)
- Security Expert: supporting all phases of a SDLC
Agenda

1. Security, Trust, and Compliance of Business Processes
2. Process-aware Information Systems
3. Research Directions and Challenges
4. Conclusion
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
Compliance and Additional Requirements

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. Security, Trust, and Compliance of Business Processes
2. Process-aware Information Systems
3. Research Directions and Challenges
4. 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)
How the Future Might Look Like

Customer
On Premise
Log

Kostenverwaltung
(z.B. Concur)
Log

Human Resources
(z.B. SuccessFactors)
Log

CRM
(z.B. Salesforce)
Log
Evolution of Source Code

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

![Bar chart showing the number of systems and customers over time from 1998 to 2012. The chart indicates a significant increase in both systems and customers in 2004.](chart.png)
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
Agenda

1 Security, Trust, and Compliance of Business Processes
2 Process-aware Information Systems
3 Research Directions and Challenges
4 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. Security, Trust, and Compliance of Business Processes
2. Process-aware Information Systems
3. Research Directions and Challenges
4. 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!
Wihem Arsac, Luca Compagna, Giancarlo Pellegrino, and Serena Elisa Ponta. 
Security validation of business processes via model-checking.
In Úlfar Erlingsson, Roel Wieringa, and Nicola Zannone, editors, ESSoS, volume 6542 of 

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 (Inbip), 

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 
