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

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

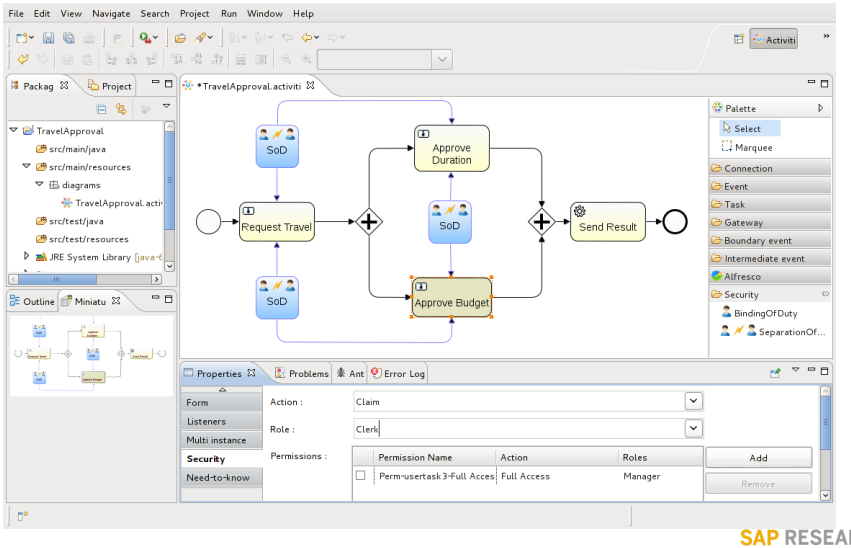
Observations:

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

Agenda

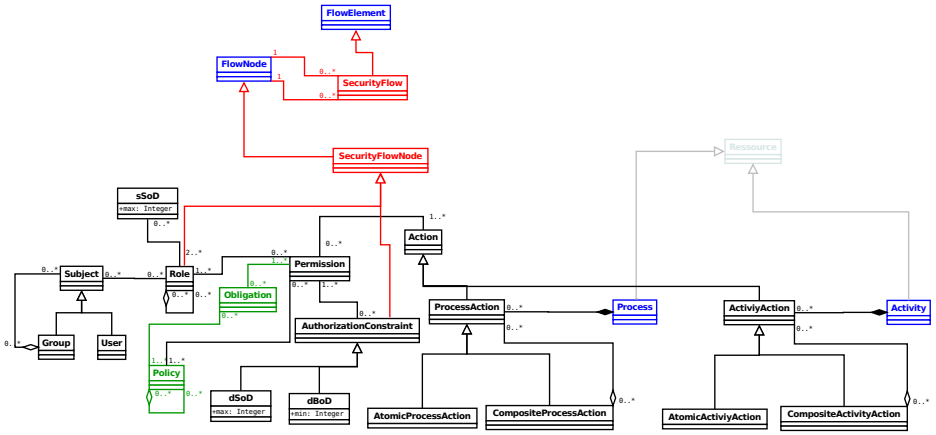
Secure Business Processes

A Simple Example: A Travel Approval Process



The SecureBPMN Meta-Model

A Meta-model-based Extension of BPMN



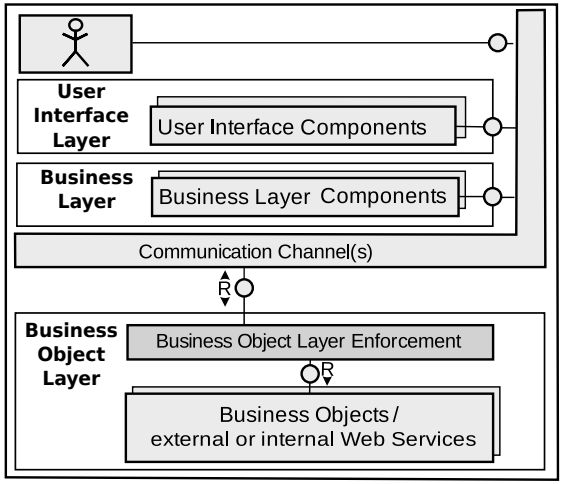
- Hierarchical RBAC
- Fine-grained SoD/BoD
- Need to know
- Break-glass support
- Delegation
- . . .

SAP RESEARCH

Modern Business Process Execution

Cloud- or SoA-based Business Process Execution

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

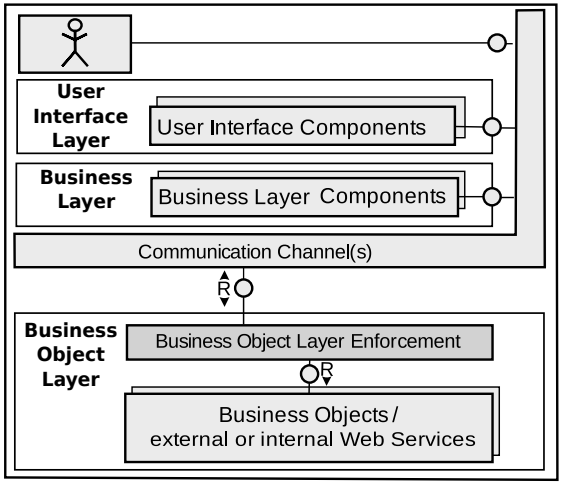


SAP RESEARCH

Modern Business Process Execution

Cloud- or SoA-based Business Process Execution

- PBMSs integrate many (technical) layers
- Security needs to 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



SAP RESEARCH

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`)

SAP RESEARCH

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 + "’;"
```

SAP RESEARCH
© 2012 SAP AG. All Rights Reserved.
Page 8 of 18

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"
```

SAP RESEARCH
© 2012 SAP AG. All Rights Reserved.
Page 8 of 18

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’;"
```

SAP RESEARCH
© 2012 SAP AG. All Rights Reserved.
Page 8 of 18

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”!

SAP RESEARCH

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

SAP RESEARCH

Agenda

SAP RESEARCH

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):

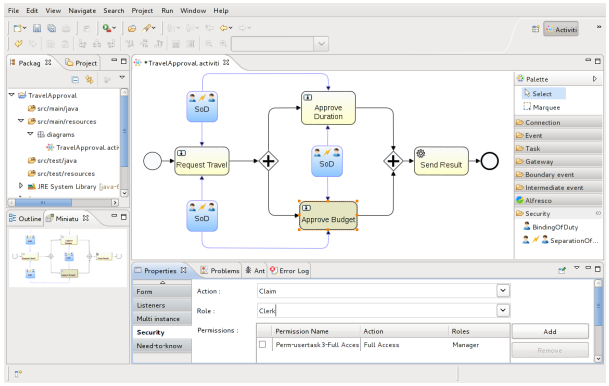
- Access control: check presence of access control checks (e. g., PEPs)
- Separation of Duty: check control flow
- Need to Know: check access to process variables or messages and derived data (data flow as well as control flow)

SAP RESEARCH

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" writable="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

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.

© 2012 SAP AG. All rights reserved

