SECURING PROCESSES FOR OUTSOURCING INTO THE CLOUD

Sven Wenzel¹, Christian Wessel¹, Thorsten Humberg², Jan Jürjens¹,²

¹tu technische universität dortmund ²Fraunhofer ISST

CloudSecGov, 19.4.2012

© Fraunhofer ISST
Overview

Process

Cloud

Risk analysis

Compliance analysis

Security analysis

Toolsupport: CARiSMA
Cloud Computing

- Most common definition: „The NIST Definition of Cloud Computing“ by Peter Mell, Tim Grance
Clouds for Small and Medium-sized Enterprises (SMEs)

- Most significant advantages of cloud computing
  - Flexibility: Less inhouse IT-infrastructure needed
  - Pay-per-use: Overhead costs can be avoided
  - Less effort for infrastructure maintenance

- Advantages are especially valid for SMEs

- But: Cloud computing is hardly used by SMEs!
Concerns regarding Cloud Computing

„I consider Cloud Computing as critical due to …“

... compliance, security and data privacy issues

... intransparent and incomparable services

... incompatible services

... non-acceptance by employees

... technologies not being fully developed yet

... difficulties integrating with existing services

... lack of know-how in IT departments

• Security
  • Confidentiality
  • Availability

• Compliance
  • Legal regulations have to be met
1: Risk analysis

- First checkup before migrating processes
- Business processes are assessed for "risky" elements
  - No consideration of probabilities of occurrence
- Identification of risks is a matching on security or compliance standards
  - E.g. BSI basic protection catalogues, ISO norms
- Various forms of input
  - Process models: UML, BPMN
  - Semi-formal: Spreadsheets
Risk analysis: Methodology

- **Input**
  1. Process descriptions in various formats
     - Converted into a simplified representation
  2. Security and Compliance patterns

- **Risk analysis searches for relations**

- **Output**
  - Matching between components and relevant patterns
Risk analysis: Determine matchings

Simple method: Text-based matchings

Text extraction → Linguistic database → Extension → Compare
Risk analysis: Results

- For each activity, relevant patterns are identified
- With a coarse rating of relevance
2. Compliance Analysis: Modelling

- Outsourcing processes might affect their compliance
- E.g. server locations matter
- Models must contain the examined aspects, e.g. role assignments for Separation of Duties (SoD)

[Diagram showing a process flow with role assignments and tasks]

[Marcel Michel 2011]
Verification of compliance properties

- Simple properties can be formulated using Object Constraint Language
  - E.g. Separation of duty

- More complex properties require more advanced techniques
  - E.g. Process fragments or temporal logic for workflow-based features

Automated verification requires detailed descriptions of both the process and the requirements.
3. Security Analysis (ongoing)

- Goal: Reveal security concerns in early design stages
- Processes and their distribution are considered

- Transfer of UMLsec annotations to business process models
Tool Support

CARiSMA

- Provides checks for the UMLsec profile
- Plugin for Eclipse
  - Integrates established modeling tools, e.g. Topcased
- Open Source
- Ongoing:
  - Implementation of SecureClouds analysis tools

http://carisma.umlsec.de
Conclusions and Outlook

- Cloud Computing for SMEs
  - Offers economic chances
  - … as well as security and compliance concerns
- The SecureClouds project supports SMEs in utilizing cloud services
  - Work is still ongoing, especially concerning security analysis and tool support

http://www.secureclouds.de
Thank you

Thorsten.Humberg@isst.fraunhofer.de
Our contribution

- Risk analysis
- Compliance analysis
- Security analysis

Process

Cloud