A FRAMEWORK FOR GENERATING USER- AND DOMAIN-TAILORED SECURITY POLICY EDITORS

Manuel Rudolph
Cornelius Moucha
Denis Feth
12.09.2016
MANUEL RUDOLPH

ABOUT ME
- **2009:** MSc Computer Science / Software Development at University of Applied Sciences, Mannheim, Germany
- **since 2009:** Employee at Fraunhofer IESE, Kaiserslautern, Germany
- **since 2013:** PhD at Technical University of Kaiserslautern, Germany

RESEARCH FIELDS
- Security Policy Specification
- User-friendly Security Solutions
- Security x Usability x Requirements Engineering
A **Security Policy** is a description of how a security system must behave in given security-related situation.

- **Other Examples**
  - Privacy – Facebook Privacy Settings: “Only friends may see my profile”
  - Data Usage Control – Business to Customer: “When business documents are sent to customers, they must be deleted after opening them 3 times or latest after 14 days”
  - Policy editors or Policy Administration Points (**PAPs**) are specification tools for security policies
Companies want their end users to specify their own security demands

But they don’t know how to provide usable security policy specification possibilities to their end users

Users do not understand policies

Policies become too complex to be handled by the end user

Users nor administrators know how to manage multiple specified and deployed security policies

(Customer statements from e.g., Bosch, Finanz Informatik, camLine, TMF e.V.)

Do you think that end users should be enabled to specify their own security policies for protecting their data in cloud services?

Yes, I think so  Yes, but end users are in most cases not capable of specifying security policies  No, end users should not be enabled to specify security policies because it would jeopardize security  No, end users need not specify any security policies

from SECCRIT User and Advisory Board survey
PROBLEM

PAPS MIGHT BE INAPPROPRIATE FOR END USERS
Different users have different security demands

An Application Domain is set of entities that have security demands and entities that can enforce security policies corresponding to the security demands.
Tailored policy editors

Stakeholder in Application Domain

Tailored policy editors
An optimized process is required for providing PAPs that are

- better tailored to application domain
  - domain-specific, understandable terminology
  - expressiveness limited to domain requirements

- better tailored to policy author
  - better guidance during specification process
  - expressiveness limited to policy authors’ skill level
  - better visualization/explanation of effects

Process contains automation during the tailoring in some parts for

- faster adaption to new scenarios and modification of existing one ➔ less needed development time
DEFINITIONS SLP AND ILP

A **Specification Level Policy** is a human-understandable representation of one or more security requirements of the domain and describes the implementation of security measures from the perspective of the policy author.

An **Implementation Level Policy** is a (organizationally and/or technically) enforceable security policy. ILPs target the concrete persons or systems that enforce the policy and contain all information that are required for the enforcement by the target group or system.

I want to understand and specify SLPs
Policy Author

I want to understand and enforce ILPs
System
A **Specification Level Policy Template** is a blueprint of a SLP that is not completely instantiated. The instantiation of variable parts done during specification generates a concrete SLP.

An **Implementation Level Policy Template** is a blueprint of an ILP that is not completely instantiated. The instantiation of variable parts based on the instantiation of the corresponding SLP generates an ILP.
DEFINITIONS SLPT AND ILPT

Vocabulary Model Instance

<table>
<thead>
<tr>
<th>SLPT Specification Level Policy Template</th>
<th>is manually instantiated by policy author to</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILPT Implementation Level Policy Template</td>
<td>is refined to (transformation rules specified by method expert)</td>
</tr>
</tbody>
</table>

Target Audience: Policy Author

<table>
<thead>
<tr>
<th>SLP Specification Level Policy</th>
</tr>
</thead>
</table>

Target Audience: Enforcing Entity

<table>
<thead>
<tr>
<th>ILP Implementation Level Policy</th>
</tr>
</thead>
</table>

I want to understand and specify SLPs

WHAT

I want to understand and enforce ILPs

HOW
**EXAMPLES**

**Policy C17: Loss of LAN connectivity alert**

<table>
<thead>
<tr>
<th>ID</th>
<th>Policy</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>C17</td>
<td>Loss of LAN connectivity alert</td>
<td>LAN connectivity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Architectural Level</th>
<th>Policy Creator</th>
<th>Security Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>cloud infrastructure level</td>
<td>cloud infrastructure provider</td>
<td>availability</td>
</tr>
</tbody>
</table>

**Policy: Template System**

If the network connection of the DB server [SQL Server | Commssmain] is lost, then notify <email address> via email, write a log entry, write a notification and make a log entry, if the DB server is connected again, show notifications on the user interface (for facility [AMARIS Austria | AMARIS Italy] with severity: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10)+.

**Description:**

One of the centerpiece of Cloud infrastructure is Local Area Network access. It provides connectivity to all Hosts and VMs. If any Host loses LAN connectivity (due to misconfigurations or hardware failures), some action must be taken by the cloud provider to restore LAN connectivity.

**Threat:**

Loss of network connectivity, e.g., due to misconfiguration, hardware failures, etc. (SECURITY13: BNA-3)

**Exemplary Instantiation:**

If the network connection of the DB server SQL Server is lost, then notify manuel.rudolph@iese.fraunhofer.de via email, write a notification and make a log entry, if the DB server is connected again and show notifications on the user interface (for facility AMARIS Italy with severity: 5).

---

**SLPT**

If the network connection of the DB server SQL Server is lost, then notify manuel.rudolph@iese.fraunhofer.de via email, write a notification and make a log entry, if the DB server is connected again and show notifications on the user interface (for facility AMARIS Italy with severity: 5).

---

**ILPT**

```xml
<lowLevelGroup id="t2_countermeasure_blocks_connection_back">
  <lowLevelBlock id="t2_countermeasure_blocks_connection_back_notification" use="t2_countermeasure_blocks_connection_back_notification">
    <linkInd2use:executeAction name="urn:action:Ind2use:smar:senMail">
      <param:string name="msgPlain" value="Dear Customer, I\n\nwe detected that the network connection of DB server &lt;&lt;DB Server Name&gt;&gt; is lost. I\n\nplease use email to contact us at &lt;&lt;mail address&gt;&gt; for further information. (for facility [AMARIS Austria | AMARIS Italy] with severity: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10)+. &lt;&lt;(message body)\n\nBest Regards, &lt;&lt;Signature&gt;&gt;">
      <param:string name="msgHTML" value="&lt;html&gt;&lt;head&gt;&lt;title&gt;IND2UCE Policy Violation Mail&lt;/title&gt;&lt;/head&gt;&lt;/html&gt;&lt;body&gt;Dear Customer, &lt;b&gt;we detected that the &lt;b&gt;network connection &lt;i&gt;of your &lt;i&gt;DB server&lt;i&gt;&lt;/b&gt; is connected again!&lt;/i&gt;&lt;/b&gt;&lt;/i&gt;&lt;/i&gt; &lt;i&gt;&lt;message body&gt;&lt;/i&gt;&lt;/body&gt;&lt;/html&gt;"/>
      <param:boolean name="ind2uceLogo" value="true"/>
      <param:string name="subject" value="Policy Violation Back to normal"/>
      <param:string name="recipient" value="manuel.rudolph@iese.fraunhofer.de"/>
      <executeAction name="urn:action:ind2uceextra_push"/>
    </linkInd2use:executeAction>
    <executeAction name="urn:action:ind2uceextra_push"/>
  </lowLevelBlock>
</lowLevelGroup>
```

**ILP**

```xml
<param:string name="msgHTML" value="&lt;html&gt;&lt;head&gt;&lt;title&gt;IND2UCE Policy Violation Mail&lt;/title&gt;&lt;/head&gt;&lt;/html&gt;&lt;body&gt;Dear Customer, &lt;b&gt;we detected that the &lt;b&gt;network connection &lt;i&gt;of your &lt;i&gt;DB server&lt;i&gt;&lt;/b&gt; is connected again!&lt;/i&gt;&lt;/b&gt;&lt;/i&gt; &lt;i&gt;&lt;message body&gt;&lt;/i&gt;&lt;/body&gt;&lt;/html&gt;"/>
```
MODEL AND VOCABULARY

- **Security Policy Model** Instantiation and Security Policy Vocabulary Extraction

<table>
<thead>
<tr>
<th>Intellectual Property</th>
<th>Unauthorized Access to sensitive data</th>
<th>Encrypt IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mails</td>
<td>Modification of content</td>
<td>Sign all emails</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>Unallowed Relocation</td>
<td>Migration to secure location</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Malware Attack</td>
<td>All mobile devices must have safeguards</td>
</tr>
<tr>
<td>Servers</td>
<td>Too high load</td>
<td>Inform the administrator</td>
</tr>
</tbody>
</table>

Elicited Information from Application Domain

Security Policy Model

Security Policy Vocabulary

Method Expert

© Fraunhofer IESE
PAP FRAMEWORK

■ PAP generation

View layer: Platform Components and Editor
- Android
- Swing
- Web

Presentation layer: Policy Specification Paradigms
- Security Policy Templates
- Composition of Predefined Policy Blocks
- Selection from List of Predefined Policies

Model layer: Security Policy Vocabulary Instance
- Cloud Infrastructure
- Financial Advisor App
- Data Classification

Low Level Policy Language: Instantiation Rules
- IND²UCE Language (XACML)
- ...
A **Policy Specification Paradigm** defines an interaction concept and process for the specification of security policies or the instantiation of SLPTs in a PAP.
Selection of PAP wrt. Policy Specification Paradigm

- Predefined Set of Security Policies
- Selection from List of Predefined Policies
- Policy Template Instantiation
- Policy Specification Wizard
- Composition of Predefined Policy-Blocks
- Plain Text Security Policy Specification

Security Policy Specification Paradigms
POLICY ADMINISTRATION POINT FRAMEWORK EXAMPLE (1)

**PAP Framework**

- **View layer:** Platform Components and Editor
  - Android
  - Swing
  - Web
- **Presentation layer:** Policy Specification Paradigms
  - Security Policy Templates
  - Composition of Predefined Policy Blocks
  - Selection from List of Predefined Policies
- **Model layer:** Security Policy Vocabulary Instance
  - Cloud Infrastructure
  - Financial Advisor App
  - Data Classification
- **Low Level Policy Language:** Instantiation Rules
  - IND²UCE Language
    - (XACML)
  - ...

**Exemplary SWING PAP (1)**
POLICY ADMINISTRATION POINT FRAMEWORK EXAMPLE (2)

- PAP Framework

- Exemplary SWING PAP (2)
POLICY ADMINISTRATION POINT FRAMEWORK
EXAMPLE (3)

- PAP Framework
  - View layer:
    - Platform Components and Editor
  - Presentation layer:
    - Policy Specification Paradigms
  - Model layer:
    - Security Policy Vocabulary Instance
  - Low Level Policy Language:
    - Instantiation Rules

- Exemplary SWING PAP (3)
  - Policy Specification Paradigms
  - Security Policy Templates
  - Composition of Predefined Policy Blocks
  - Selection from List of Predefined Policies
  - Cloud Infrastructure
  - Financial Advisor App
  - Data Classification
  - Low Level Policy Language:
    - Instantiation Rules
  - PAP Framework Core Module
  - VM Network Connection:
    - Critical VM Migration
    - VM Network Connection
    - Virtual Machine CPU Load
    - Choice of Policies
    - Examples:
      - If the network connection of the DB server is lost, then notify
        christian.jung@iese.fraunhofer.de via email and show notifications on the user interface
        (for facility AMARIS Austria with severity: 3).
        - manual_rudolph@iese.fraunhofer.de via email, write a log entry, write a notification and
          make a log entry if the DB server is connected again and show notifications on the user
          interface (for facility AMARIS Italy with severity: 5).
      - If the network connection of the DB server is lost, then write a log entry.
PAP Framework

View layer:
- Platform Components and Editor
- Android
- Swing
- Web

Presentation layer:
- Security Policy Templates
- Composition of Predefined Policy Blocks
- Selection from List of Predefined Policies

Model layer:
- Cloud Infrastructure
- Financial Advisor App
- Data Classification

Low Level Policy Language:
- IND²UCE Language

Low Level Policy Language:
- Instantiation Rules

Exemplary Android PAP (1)

- Secure E-Mail-Message
- Secure E-Mail-Message
- E-Mail-Access
- Secure E-Mail-Message
- Security Awareness
- Data Classification

- Free exchange of data
- Access to Redaction system
- Right to access to public data
- Availability of public data
- Access to customer data
- First access to customer data
- Protection areas
- Anomaly detection
- Samples

PAP Framework Core Module

Passwort for the Redaction system
- \( \text{contain at least 5} \)
- \( \text{min. 6} \) Sonderzeichen
- \( \text{contain at least } \) Zahlen
- \( \text{contain at least } \)
- \( \text{contain at least } \) Groß- und Kleinschreibung
- \( \text{expire after } \) Tage

POLICY ADMINISTRATION POINT FRAMEWORK
EXAMPLE (4)

© Fraunhofer IESE
PAP Framework

- View layer: Platform Components and Editor
- Android
- Swing
- Web

- Presentation layer: Policy Specification Paradigms
- Security Policy Templates
- Composition of Predefined Policy Blocks
- Selection from List of Predefined Policies

- Model layer: Security Policy Vocabulary Instance
- Cloud Infrastructure
- Financial Advisor App
- Data Classification

- Low Level Policy Language: Instantiation Rules
- IND²UCE Language (XACML)
- ... (space for additional explanation)

- Low Level Policy Language: Instantiation Rules

- PAP Framework Core Module

Exemplary Android PAP (2)

- Critical VM Migration
- VM Network Connection
- Virtual Machine CPU Load

Text in the mobile app:
- If a critical virtual machine is moved to a host already running a critical VM, then notify manu@manu.de via email.
- If a critical virtual machine is moved to a host not yet running a critical VM and write a log entry.
PAPIF EXAMPLE (6)

**PAP Framework**

- **View layer:** Platform Components and Editor
  - Android
  - Swing
  - Web

- **Presentation layer:** Policy Specification Paradigms
  - Security Policy Templates
  - Composition of Predefined Policy Blocks
  - Selection from List of Predefined Policies

- **Model layer:** Security Policy Vocabulary Instance
  - Cloud Infrastructure
  - Financial Advisor App
  - Data Classification

- **Low Level Policy Language:** Instantiation Rules
  - IND²UCE Language (XACML)

- **Low Level Policy Language:** Instantiation Rules

**Exemplary Web PAP**

- **Ind2uce PAP Setup your policy**
  - Critical VM Migration
  - VM Network Connection
  - Virtual Machine CPU Load
  - Policy ID: 1

- **Policy:**
  - If a critical virtual machine is moved to a host already running a critical VM, then
    - move virtual machine to a host not yet running a critical VM
    - notify manu@manu.de via email
    - write a log entry
    - show notifications on the user interface

- **Code snippet (XACML):**

```xml
<policy xmlns="http://www.iese.fhg.de/ind2uce/1.1/enforcementlanguage"
  xmlns:ns1="http://www.iese.fhg.de/ind2uce/1.1/enforcementlanguage"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:par="http://www.iese.fhg.de/ind2uce/1.1/parameter" xmlns:ns1:par="http://www.iese.fhg.de/ind2uce/1.1/pap"
  name="Critical_VM_Migration">
  <detectionMechanism name="Migrate"/>
  <description/>
  <condition>
    <trigger action="vm.event:Ind2uce:VM.MigratedEvent" isTrig="true">
      <paramstring name="method" value="criticalServiceEnabled"/>
      <paramstring name="host" value="true"/>
      <paramstring name="ignoreM" value="false"/>
    </trigger>
  </condition>
</policy>
```
Generated **ILP** for SLP: If the network connection of the DB server SQL Server is lost, then notify manuel.rudolph@iese.fraunhofer.de via email, write a notification and make a log entry, if the DB server is connected again and show notifications on the user interface (for facility AMARIS Italy with severity: 5).
Sicherheitsrichtlinie

WENN der Kundenberater auf Kundendaten zugreifen will und innerhalb 5 Minuten schon auf 10 Datensätze von unterschiedlichen Kunden zugegriffen hat und sich außerhalb der Bank befindet, dann verbiete den Zugriff und informiere den Vorgesetzten per E-Mail: test@mail.de.

Maschinenlesbare Sicherheitsrichtlinie

<?xml version="1.0" encoding="utf-8"?>
  <preventiveMechanism name="scenario04_79000218">
    <timestep amount="10" unit="SECONDS" />
    <trigger action="RequestClientData" isTry="true">
      <trigger>
        <condition>
          <not>
            <pip:boolean name="context" default="false">
              <param:string name="value" value="WorkingInBank" />
            </pip:boolean>
          </not>
          <not>
            <replimit amount="5" unit="MINUTES" lowerlimit="0" upperlimit="10">
              <eventMatch action="RequestClientData" isTry="true"/>
            </replimit>
          </not>
        </and>
      </condition>
      <inhibit/>
      <executeAction name="SendMail">
        <param:string name="rct_to" value="test@mail.de" />
        <param:string name="body" value="Too many accesses on customer data." />
        <param:string name="subject" value="IND2UCE Info" />
      </executeAction>
      <authorizationAction />
    </preventiveMechanism>
  </policy>
CONCLUSION

- Framework for generating tailored policy editors
- Future work
  - more specification paradigms need to be integrated and evaluated
  - further elaboration of policy model
- One generated policy editor was evaluated (see paper)
Thank you for your attention!