Architectural Access Control Policy Refinement and Verification under Uncertainty

Sebastian Hahner
15th European Conference on Software Architecture (ECSA’21) – Doctoral Symposium
Motivation

Confidentiality requirement: Personal data is only allowed to be stored and processed on European servers or servers with “an adequate level of protection” [GDPR, Art. 45]
Motivation

There are different types of uncertainty in architectural modeling

How to deal with the impact of uncertainty on confidentiality?
The Topic, Summarized

Architectural Access Control Policy Refinement and Verification under Uncertainty

High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)
The Topic, Summarized

Architectural Access Control Policy Refinement and Verification under Uncertainty

High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Uncertainty
(e.g., in structure or environment)

Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)
## Research Questions and Contributions

<table>
<thead>
<tr>
<th>Research Questions</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) How to treat uncertainty on different abstraction levels and in varying context regarding its impact on confidentiality?</td>
<td>▪ <strong>Metamodel</strong> for architecture-level access control policies under uncertainty</td>
</tr>
<tr>
<td>2) How to refine high-level confidentiality requirements based on architectural modeling?</td>
<td>▪ <strong>Uncertainty impact analysis</strong> of architectural design decisions on confidentiality</td>
</tr>
<tr>
<td>3) How to verify refined policies against system architectures while considering uncertainty?</td>
<td>▪ Uncertainty-aware, design-time access control policy <strong>refinement</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Policy <strong>verification</strong> based on adapting existing architecture-level confidentiality analyses [Seifermann19]</td>
</tr>
</tbody>
</table>

Approach

- Extend the Palladio ADL with means to model uncertainty and access control policies
- Define uncertainty impact analysis on confidentiality with propagation of uncertainty in architectural design decision
- Refine and verify high-level access control policies
  - Use the results of the uncertainty impact analysis to identify critical decisions
  - Use the information from the modeled architecture (e.g., structure and behavior) to refine policies that can be verified under remaining uncertainty

Evaluation

Evaluation Goals

- **Expressiveness** of the architecture-level modeling of policies under uncertainty
- **Correctness** of the uncertainty-aware policy refinement process
- **Accuracy** of the uncertainty impact analysis for confidentiality
- **Accuracy** of the verification of access control policies under uncertainty

Evaluation Approach

- Use different access control models and existing uncertainty taxonomies [Perez-Palacin14]
- Conduct a formal proof, e.g., by formalizing systems and policies and verifying the implication relation
- Use existing systems with crucial confidentiality requirements as case study, e.g., the open-source contact tracing app *Corona-Warn-App* [RKI21]

---

Related Work

High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Access Control Policy Refinement

Uncertainty Impact Analysis

Uncertainty
(e.g., in structure or environment)

Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)
Related Work

High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Access Control Policy Refinement

Uncertainty Impact Analysis

Related: Uncertainty in architectural modeling


Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)

Uncertainty
(e.g., in structure or environment)
Related Work

High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)

Access Control Policy Refinement

Uncertainty Impact Analysis

Uncertainty
(e.g., in structure or environment)


High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)

Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)

Access Control Policy Refinement

Uncertainty Impact Analysis

Uncertainty
(e.g., in structure or environment)

Related Work

High-Level Confidentiality Requirements (e.g., based on SLAs, or the GDPR)

Access Control Policy Refinement

Uncertainty Impact Analysis

Low-Level Access Control Policies (e.g., based on RBAC or ABAC)

Related: Uncertainty in architectural modeling

[Noppen08] [Esfahani13]

Related: Uncertainty in policy refinement

[Su05] [He09]

Related: Uncertainty-aware access control

[Hengartner07] [Bures20]
Conclusion

Problem

- Gap between high-level confidentiality requirements and access control policies
- Imprecise early confidentiality assessment due to abstraction and uncertainty

Research Questions

- Impact of uncertainty on confidentiality?
- Refinement of confidentiality requirements to access control policies?
- Verification of refined policies while considering uncertainty?

Diagram:

- Database System A
- Database System B
- Non-European Server
- «deploy»
References