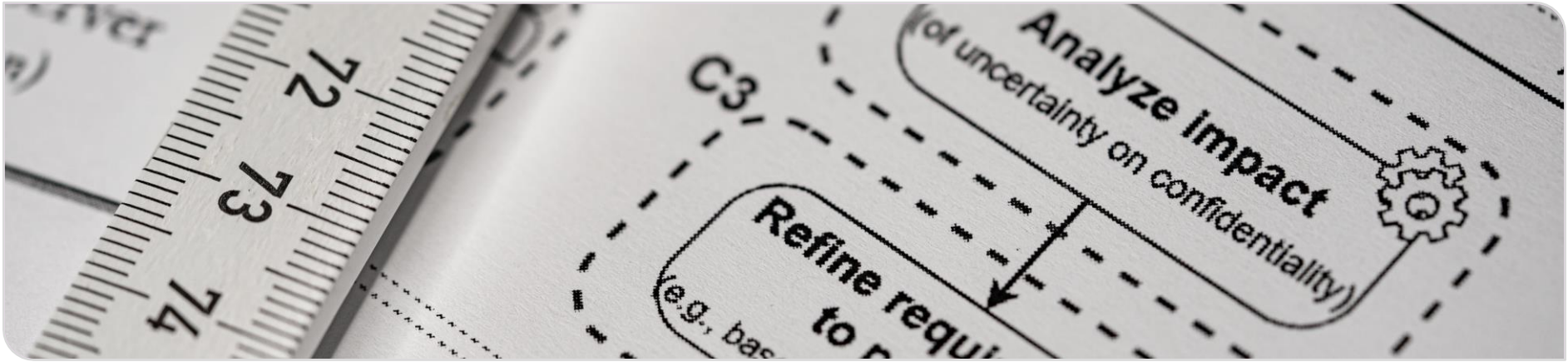
Karlsruhe Institute of Technology

Architectural Access Control Policy Refinement and Verification under Uncertainty

Sebastian Hahner

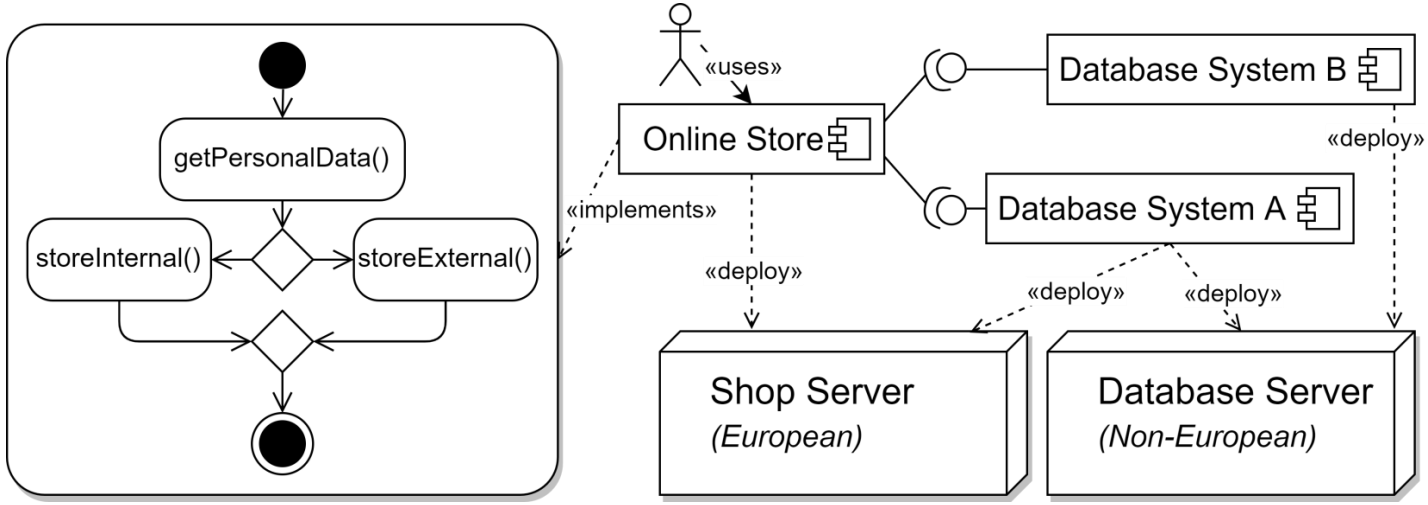
15th European Conference on Software Architecture (ECSA'21) – Doctoral Symposium



Motivation

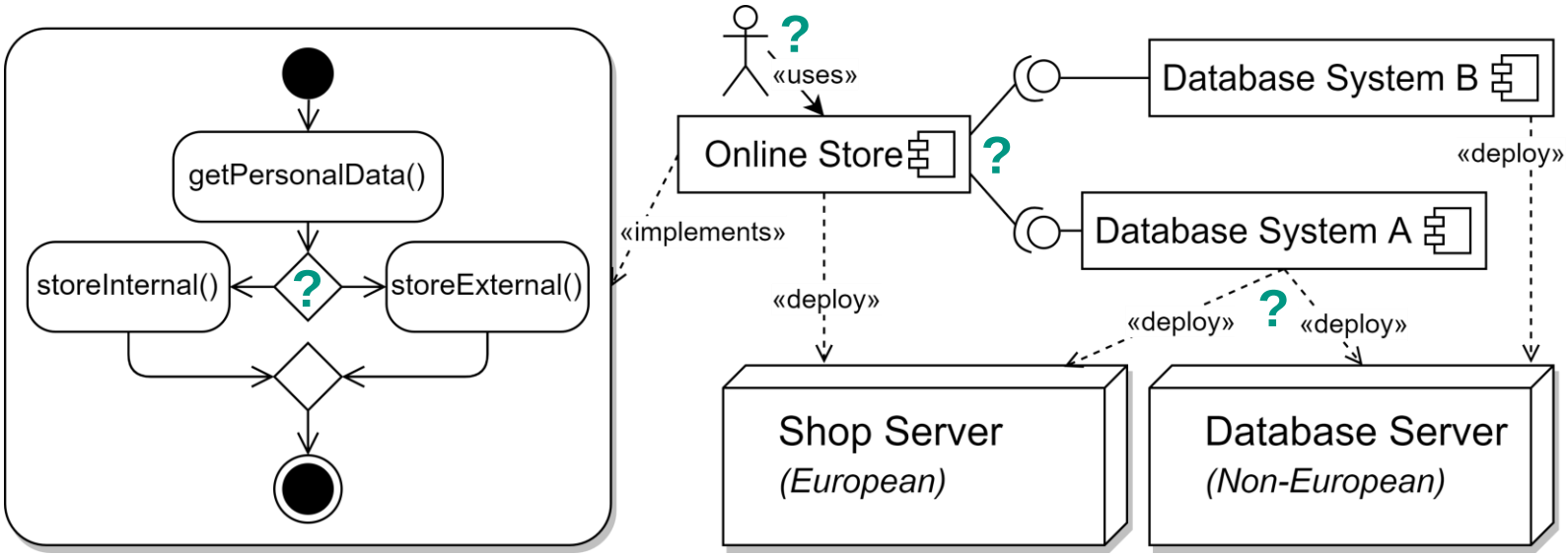
Confidentiality requirement: *Personal data is only allowed to be stored and processed on European servers or servers with “an adequate level of protection”* [GDPR, Art. 45]

How to translate and how to ensure this?



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

Research Questions

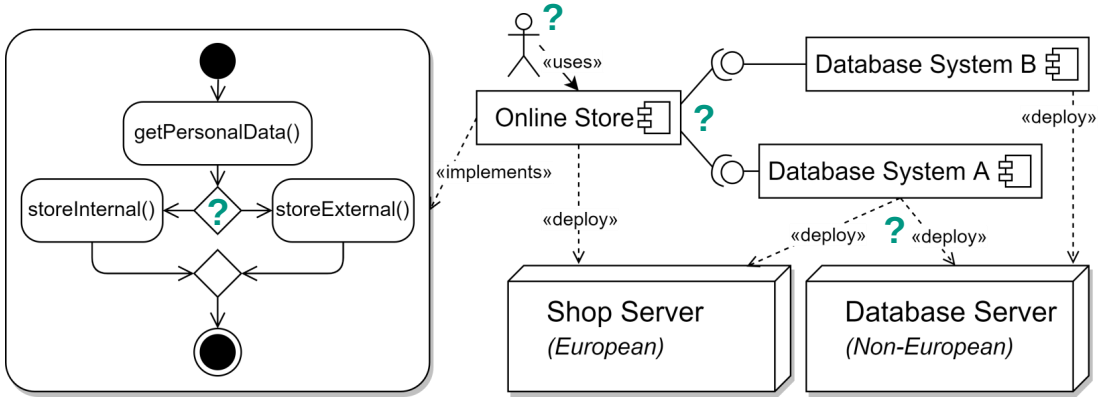
1) How to treat uncertainty on different abstraction levels and in varying context regarding its impact on confidentiality?
2) How to refine high-level confidentiality requirements based on architectural modeling?
3) How to verify refined policies against system architectures while considering uncertainty?

Contribution

- Metamodel for architecture-level access control policies under uncertainty
- Uncertainty impact analysis of architectural design decisions on confidentiality
- Uncertainty-aware, design-time access control policy refinement
- Policy verification based on adapting existing architecture-level confidentiality analyses [Seifermann19]

[Seifermann19] S. Seifermann, et al., Data-driven software architecture for analyzing confidentiality, in: ICSA, 2019, p. 1–10.

Approach



- Extend the Palladio ADL [Reussner16] 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

[Reussner16] R. H. Reussner, et al., Modeling and Simulating Software Architectures: The Palladio Approach, The MIT Press, 2016.

Evaluation

Evaluation Goals

- Expressiveness of the architecture-level modeling of polices 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

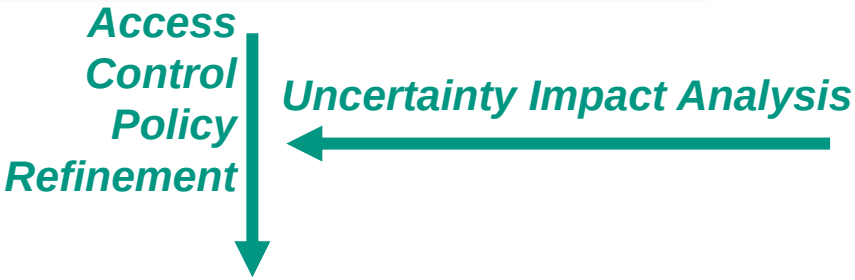
Evaluation Approach

- 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]

[Perez-Palacin14] D. Perez-Palacin, R. Mirandola, Uncertainties in the modeling of self-adaptive systems, in: ICPE, 2014, pp. 3–14.
[RKI21] Robert Koch Institute, et al., Corona-Warn-App Open-Source Project Website, 2020. URL: https://www.coronawarn.app/en

Related Work

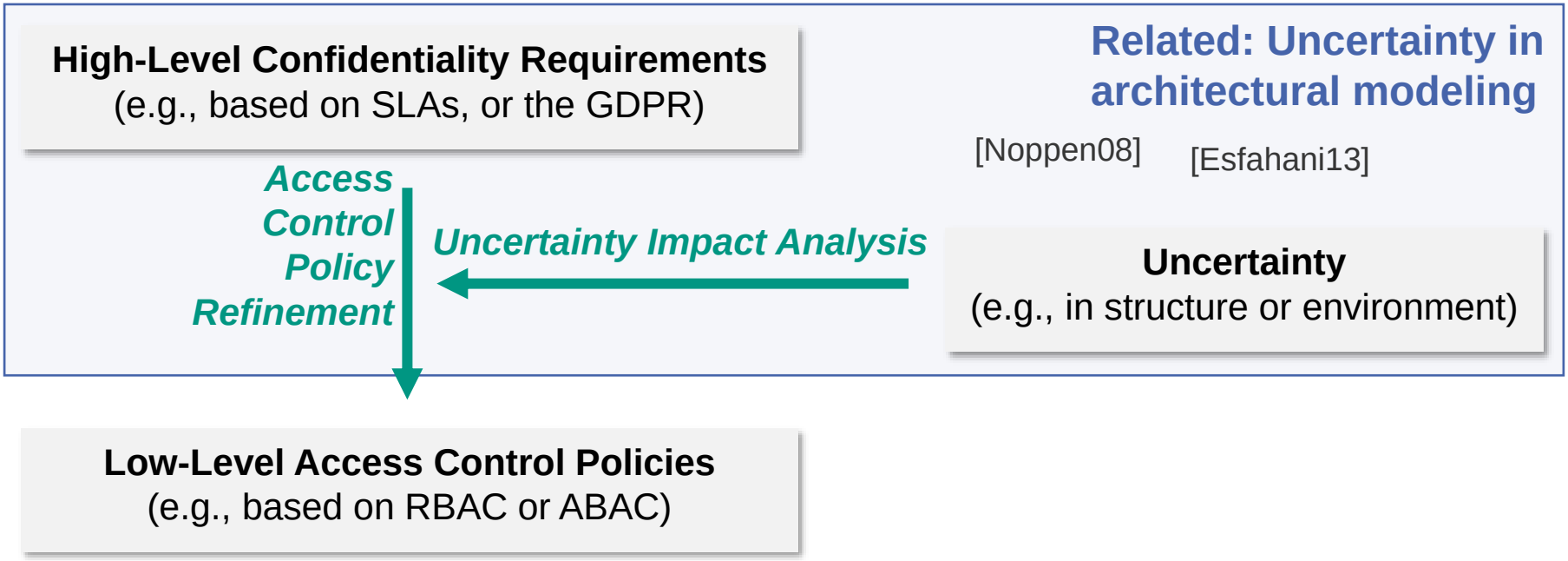
High-Level Confidentiality Requirements
(e.g., based on SLAs, or the GDPR)



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

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

Related Work



[Noppen08] Noppen, J., et al., Software development with imperfect information, Soft computing 12 (2008) 3–28. Springer.
[Esfahani13] N. Esfahani, et al., GuideArch: Guiding the exploration of architectural solution space under uncertainty, in: ICSE, 2013, pp. 43–52.

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)

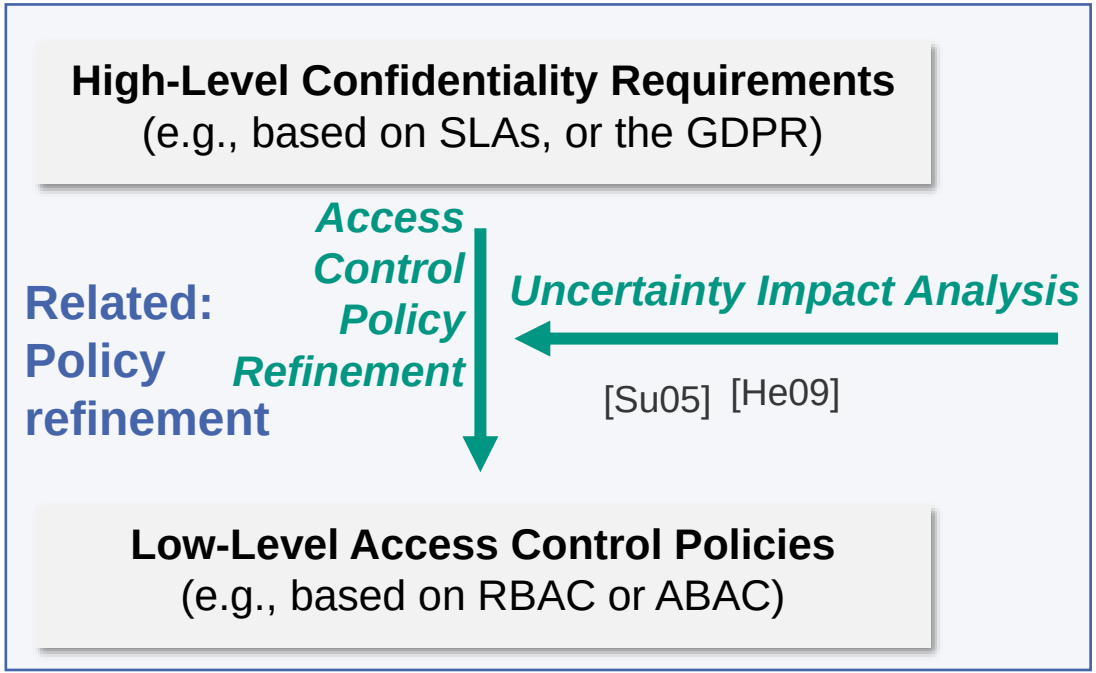
Low-Level Access Control Policies
(e.g., based on RBAC or ABAC)

[Hengartner07] [Bures20]

Related: Uncertainty-aware access control

[Hengarner07] U. Hengartner, G. Zhong, Distributed, Uncertainty-Aware Access Control for Pervasive Computing, in: PerComW, 2007, pp. 241–246.
[Bures20] T. Bures, et al., Capturing Dynamicity and Uncertainty in Security and Trust via Situational Patterns, in: Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles, Springer, 2020, pp. 295–310.

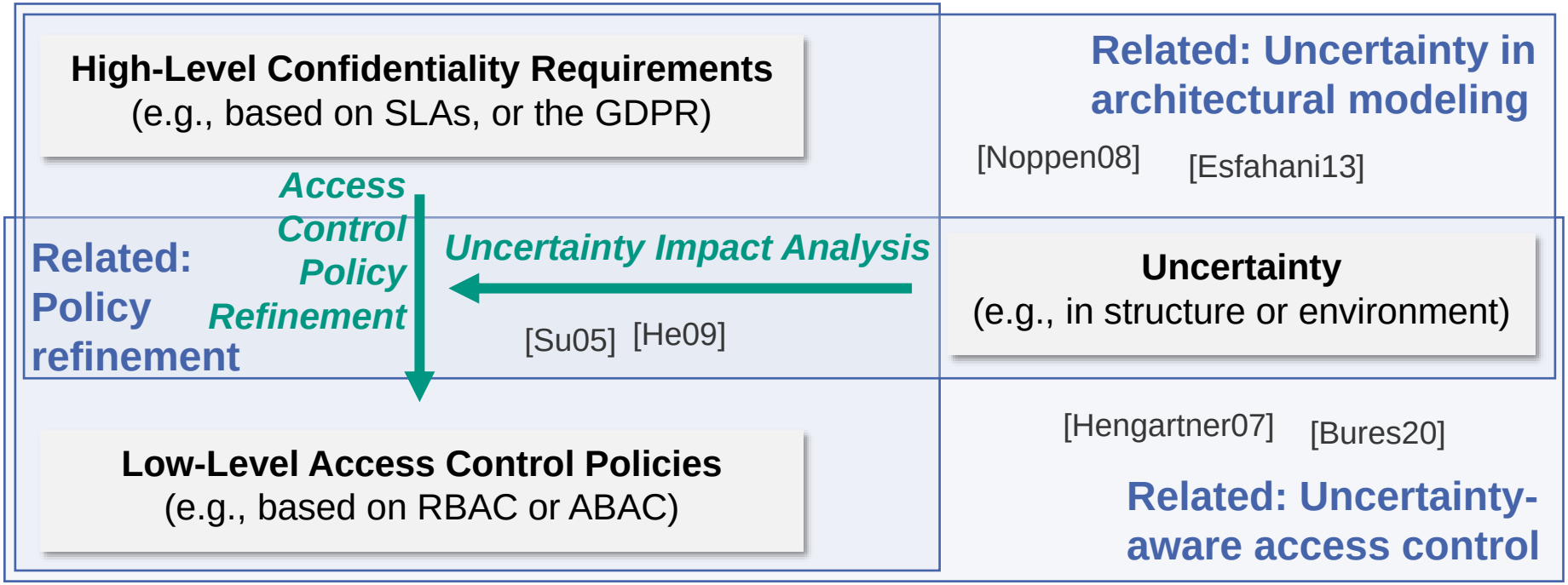
Related Work



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

[Su05] Linying Su, et al., Automated decomposition of access control policies, in: POLICY, 2005, pp. 3–13.
[He09] Q. He, A. I. Antón, Requirements-based Access Control Analysis and Policy Specification (ReCAPS), Information and Software Technology 51 (2009) 993–1009.

Related Work



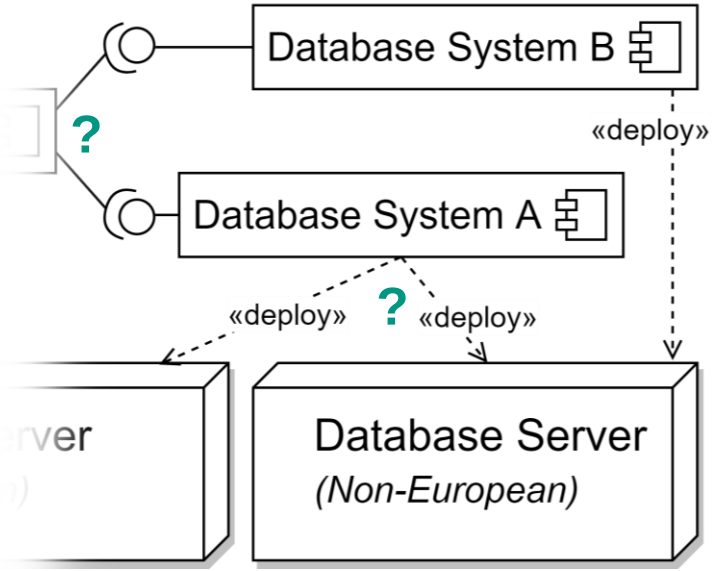
Conclusion

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?



References

- **[GDPR]** Council of European Union: REGULATION (EU) 2016/679 (General Data Protection Regulation), 2016.
- **[Seifermann19]** S. Seifermann, et al., Data-driven software architecture for analyzing confidentiality, in: ICSA, 2019, p. 1–10.
- **[Reussner16]** R. H. Reussner, et al., Modeling and Simulating Software Architectures: The Palladio Approach, The MIT Press, 2016.
- **[Perez-Palacin14]** D. Perez-Palacin, R. Mirandola, Uncertainties in the modeling of self-adaptive systems, in: ICPE, 2014, pp. 3–14.
- **[RKI21]** Robert Koch Institute, et al., Corona-Warn-App Open-Source Project Website, 2020. URL: https://www.coronawarn.app/en/, accessed 7/29/2021.
- **[Noppen08]** Noppen, J., et al., Software development with imperfect information, Soft computing 12 (2008) 3–28. Springer.
- **[Esfahani13]** N. Esfahani, et al., GuideArch: Guiding the exploration of architectural solution space under uncertainty, in: ICSE, 2013, pp. 43–52.
- **[Hengarner07]** U. Hengartner, G. Zhong, Distributed, Uncertainty-Aware Access Control for Pervasive Computing, in: PerComW, 2007, pp. 241–246.
- **[Bures20]** T. Bures, et al., Capturing Dynamicity and Uncertainty in Security and Trust via Situational Patterns, in: Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles, Springer, 2020, pp. 295–310.
- **[Su05]** Linying Su, et al., Automated decomposition of access control policies, in: POLICY, 2005, pp. 3–13.
- **[He09]** Q. He, A. I. Antón, Requirements-based Access Control Analysis and Policy Specification (ReCAPS), Information and Software Technology 51 (2009) 993–1009.