Karlsruhe Institute of Technology

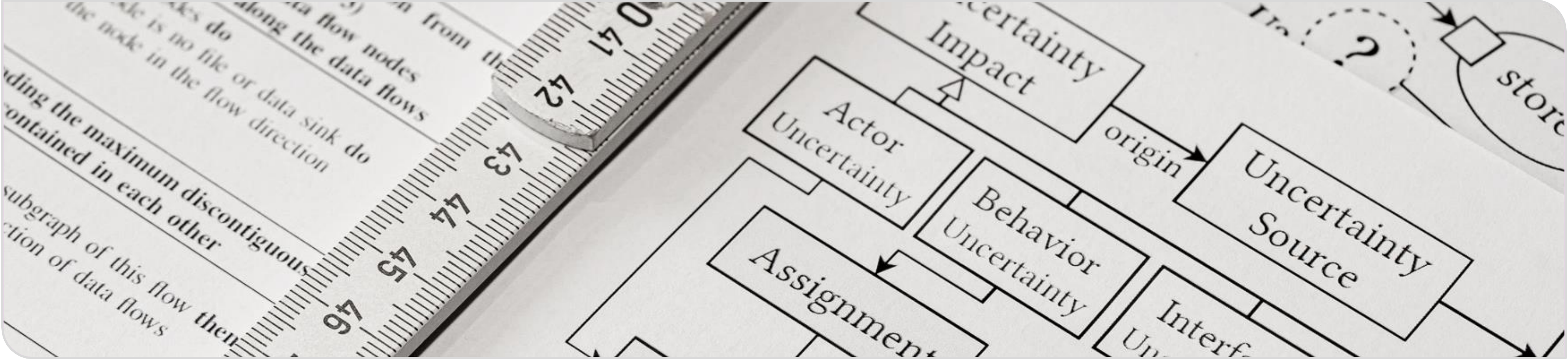
FluidTrust
Trust by fluid access control in Industry 4.0

KASTEL

Architecture-based Uncertainty Impact Analysis to ensure Confidentiality

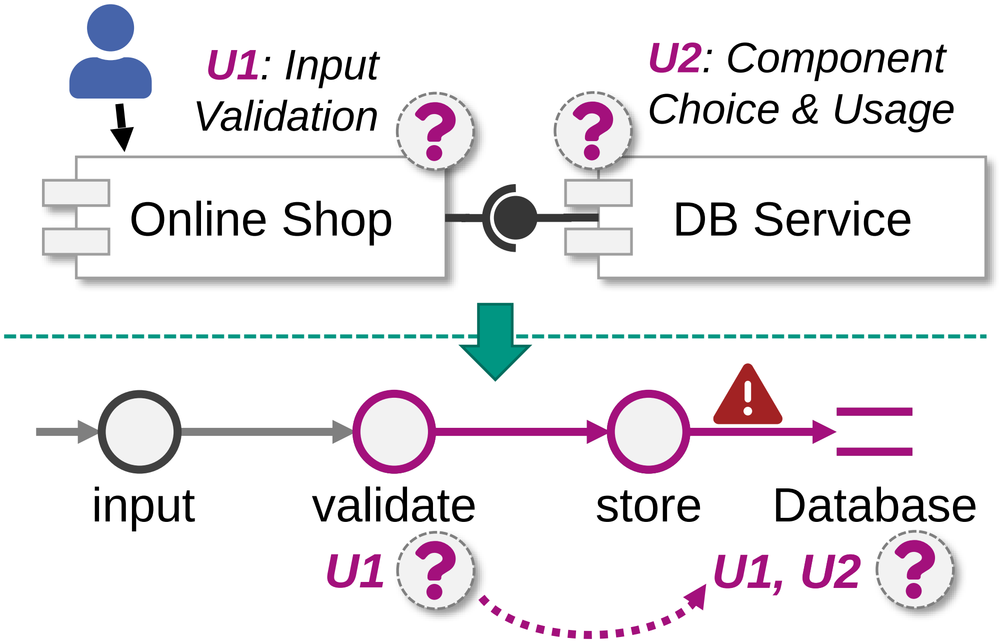
18th Symposium on Software Engineering for Adaptive and Self-Managing Systems, SEAMS’23

Sebastian Hahner, Robert Heinrich, Ralf Reussner



Motivation

- Uncertainty has an impact on a software system‘s confidentiality
  - Uncertainty sources exist in the system and its environment **[1]**
  - Design time analysis can find confidentiality violations **[2, 3]**



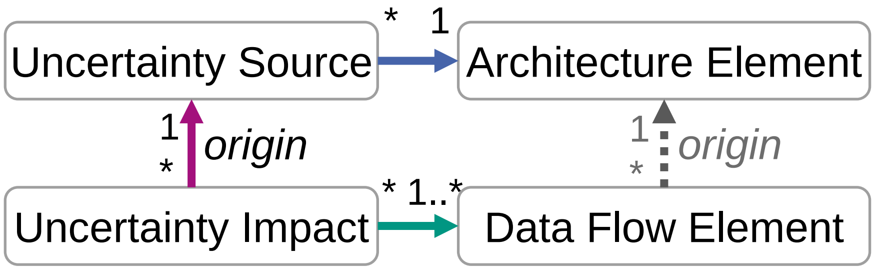
Challenges

- Uncertainty source and impact location in the system can differ
- Lack of comprehensive and precise modeling and analysis

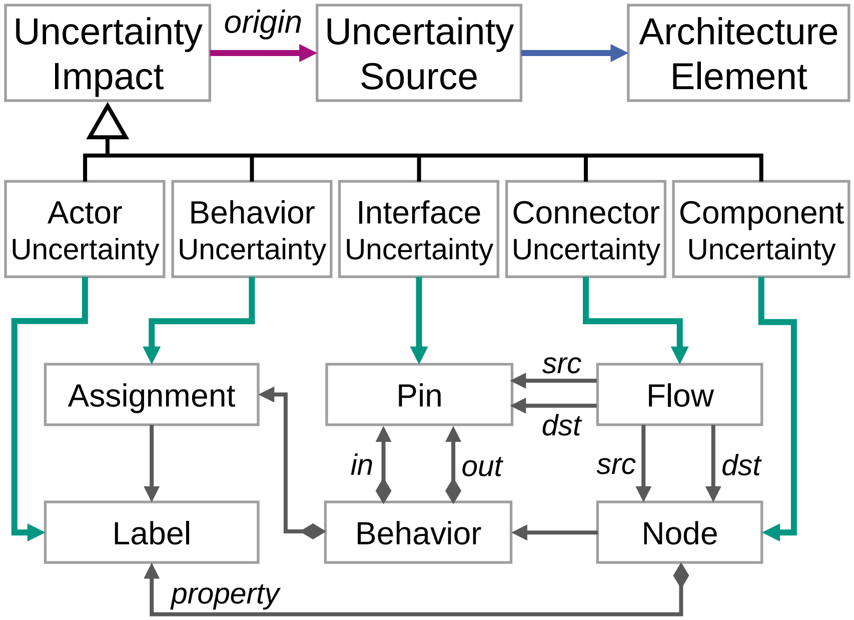
[1] M. Acosta et al., „Uncertainty in coupled models of cyber-physical systems“, In: *MODELS-C,* ACM, 2022.
[2] S. Seifermann, et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
[3] S. Hahner, et al.,”Model-based Confidentiality Analysis under Uncertainty”, In: *ICSA-C*, IEEE, 2023.

Modeling the Impact of Uncertainty on Confidentiality

- We distinguish between uncertainty sources and impact locations



- There are five uncertainty types with potential impact on confidentiality **[4]**
- We extend data flow diagrams **[5]** to represent the impact of uncertainty



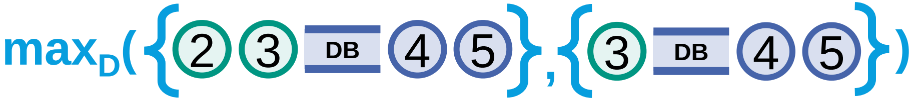
[4] S. Hahner, et al., "A Classification of Software-Architectural Uncertainty regarding Confidentiality", In: *ICETE*, Springer, 2023, accepted, to appear.
[5] S. Seifermann, et al., "A Unified Model to Detect Information Flow and Access Control Violations in Software Architectures", In: *SECRYPT*, 2021.

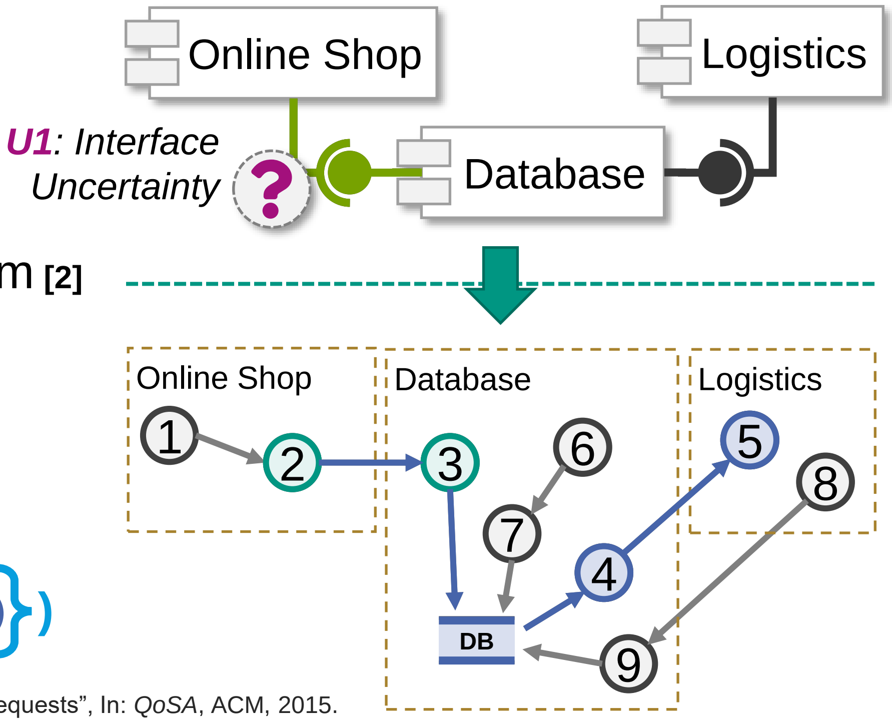
Uncertainty Impact Analysis on Confidentiality

KIT Karlsruhe Institute of Technology

Impact Analysis Algorithm

1) Annotate the uncertainty source
2) Calculate structural propagation based on change impact analysis [6]
3) Map all impacts to the data flow diagram [2]
4) Calculate the propagation along all affected data flows
5) Calculate the impact set by finding the maximum discontiguous data flows



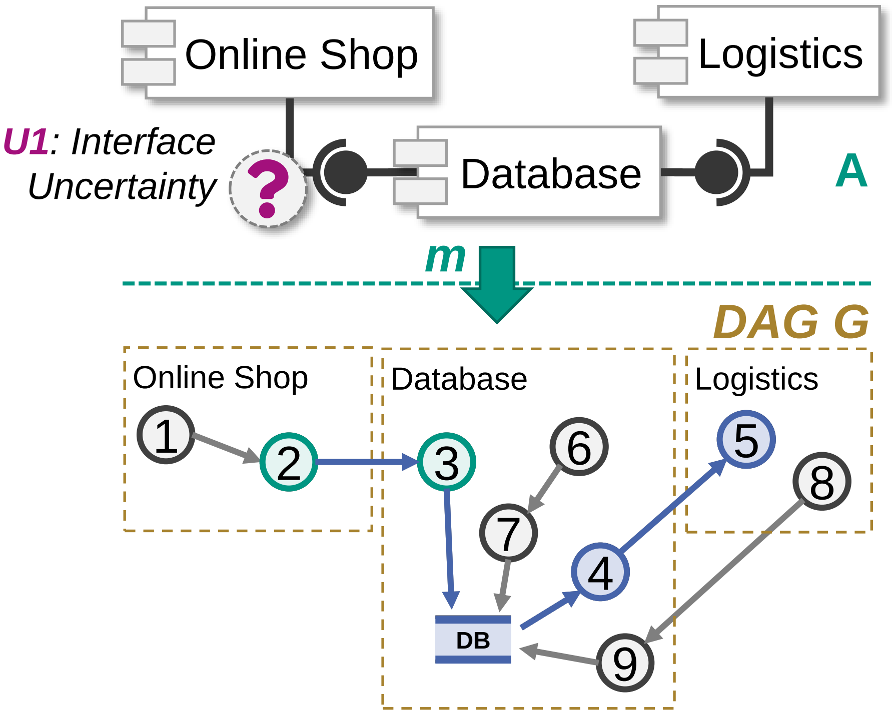


[6] K. Rostami, et al., “Architecture-based Assessment and Planning of Change Requests”, In: *QoSA*, ACM, 2015.
[2] S. Seifermann, et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.

Uncertainty Impact Analysis on Confidentiality

Formal Foundation of Impact Analysis

- Data flow diagrams can be represented as DAG G = (V, E) with a strict partial order $u \prec v$
- We reuse the mapping m(a) from the architecture A to data flow nodes
- The impact analysis of an uncertainty source S is a function $u : S \rightarrow X \subseteq V$
- The impact set is represented by an induced subgraph G[X]
- Uncertainty impacts follow the data flow: $\forall\, x \in X \subseteq V,\ \exists\, a \in A : m(a) \preceq x$



Case Study-based Evaluation

DATA SET AVAILABLE

Karlsruhe Institute of Technology

Goal Question Metric Plan

- Accuracy: How precise and complete are the calculated impact sets?
- Effort reduction: How many model elements must be considered in the analysis?

Case Study

- Corona Warn App, 19 components, 200 data flow diagram nodes
- 4 evaluation scenarios, comparing to confidentiality analysis [2]

CORONA WARN-APP

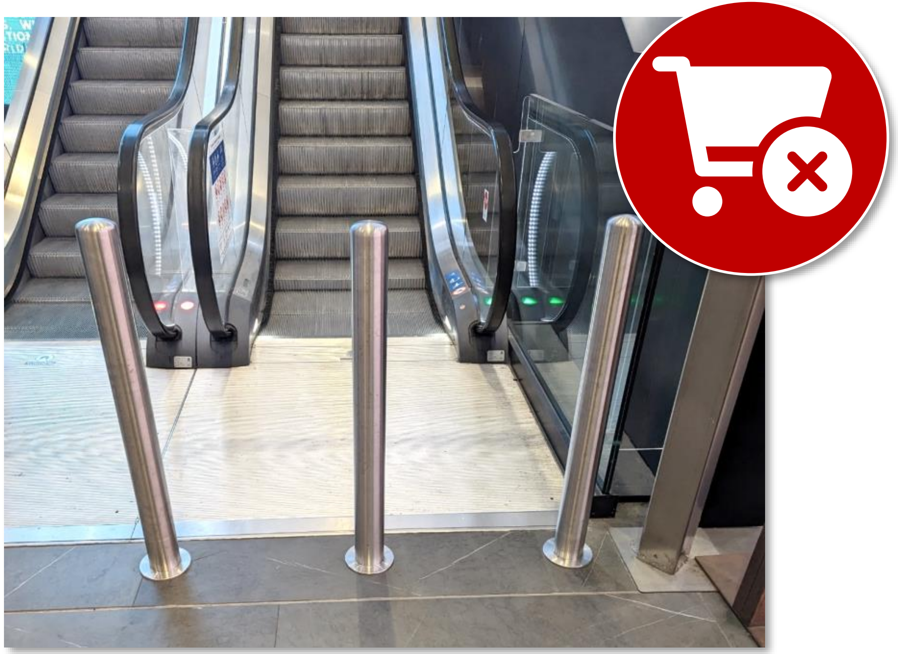
Results

- High F_1 score of *0.94*, analysis optimized for recall **R** of *1.0* without false negatives
- Impact set ratio r_i of *0.18* has slight over-estimation of affected set ratio r_a of *0.16*

	S1	S2	S3	S4	AVG
Precision P	0.838	1.000	0.840	0.882	0.890
Recall R	**1.000**	**1.000**	**1.000**	**1.000**	**1.000**
F_1 score	0.912	1.000	0.913	0.938	0.942
Ratio r_a	0.155	0.080	0.105	0.300	0.160
Ratio r_i	0.185	0.080	0.125	0.340	0.183

[2] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: *JSS*, vol. 184, 2022.

Precision vs. Recall in Security Analysis



High precision is good…

but not without high recall.

Related Work

Karlsruhe Institute of Technology

Three Categories of Related Work:

- Architecture-based uncertainty analyses use fuzzy values [7, 8] or design space exploration [9] but do not focus on confidentiality and lack precision [3]
- Uncertainty-aware confidentiality analysis also use data flow-based methods [10, 11] but require expert knowledge and lack comprehensiveness
- Uncertainty propagation for self-adaption acknowledges the analysis challenge [12], especially related to the uncertainty interaction problem [13]

[3] S. Hahner, et al.,"Model-based Confidentiality Analysis under Uncertainty", In: *ICSA-C*, IEEE, 2023.
[7] N. Esfahani, et al., "GuideArch: Guiding the exploration of architectural solution space under uncertainty", In: *ICSE*, IEEE, 2013.
[8] I. Lytra and U. Zdun, "Supporting architectural decision making for systems-of-systems design under uncertainty", In: *SESoS*, ACM, 2013.
[9] A. Koziolek, et al., "PerOpteryx: Automated application of tactics in multi-objective software architecture optimization", In: *QoSA-ISARCS*, ACM, 2011.
[10] N. Boltz, et al., "Handling environmental uncertainty in design time access control analysis", In: *SEAA*, IEEE, 2022.
[11] M. Walter, et al., "Architectural optimization for confidentiality under structural uncertainty", In: *Software Architecture*, Springer, 2022.
[12] S. M. Hezavehi, et al., "Uncertainty in self-adaptive systems: A research community perspective", In: *TAAS*, ACM, 2021.
[13] J. Cámara, et al., "Addressing the uncertainty interaction problem in software-intensive systems: challenges and desiderata", In: *MODELS*, ACM, 2022.

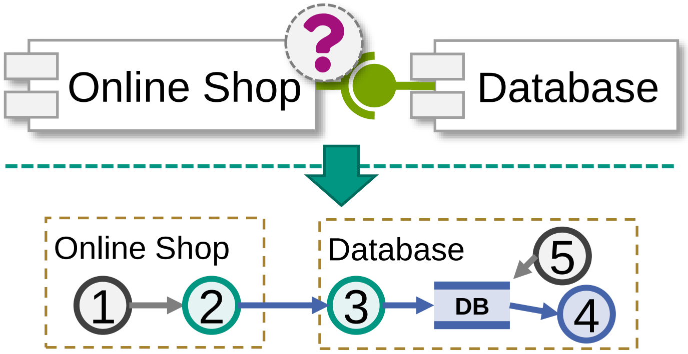
Conclusion and Future Work

- Problem: Predicting the impact of uncertainty on confidentiality
- Contribution: Modeling and analysis of the uncertainty impact by combining architecture-based and data flow-based propagation
- Benefit: More precise and less labor-intensive prediction of the potential impact of uncertainty, both at design time and run time

https://abunai.dev

Future Work

- Enhance the expressiveness of the uncertainty impact model, e.g., with variability modeling
- Combine uncertainty impact analysis with existing design time confidentiality analysis
- Extend evaluation with additional domains



References

[1] M. Acosta et al., „Uncertainty in coupled models of cyber-physical systems“, In: *MODELS-C,* ACM, 2022.

[2] S. Seifermann, et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.

[3] S. Hahner, et al.,”Model-based Confidentiality Analysis under Uncertainty”, In: *ICSA-C*, IEEE, 2023.

[4] S. Hahner, et al., “A Classification of Software-Architectural Uncertainty regarding Confidentiality”, In: *ICETE*, Springer, 2023, accepted, to appear.

[5] S. Seifermann, et al., “A Unified Model to Detect Information Flow and Access Control Violations in Software Architectures”, In: *SECRYPT*, 2021.

[6] K. Rostami, et al., “Architecture-based Assessment and Planning of Change Requests”, In: *QoSA*, ACM, 2015.

[7] N. Esfahani, et al., “GuideArch: Guiding the exploration of architectural solution space under uncertainty”, In: *ICSE*, IEEE, 2013.

[8] I. Lytra and U. Zdun, “Supporting architectural decision making for systems-of-systems design under uncertainty”, In: *SESoS*, ACM, 2013.

[9] A. Koziolek, et al., “PerOpteryx: Automated application of tactics in multi-objective software architecture optimization”, In: *QoSA-ISARCS*, ACM, 2011.

[10] N. Boltz, et al., “Handling environmental uncertainty in design time access control analysis”, In: *SEAA*, IEEE, 2022.

[11] M. Walter, et al., “Architectural optimization for confidentiality under structural uncertainty”, In: *Software Architecture*, Springer, 2022.

[12] S. M. Hezavehi, et al., “Uncertainty in self-adaptive systems: A research community perspective”, In: *TAAS*, ACM, 2021.

[13] J. Cámara, et al., “Addressing the uncertainty interaction problem in software-intensive systems: challenges and desiderata”, In: *MODELS*, ACM, 2022.