Karlsruhe Institute of Technology

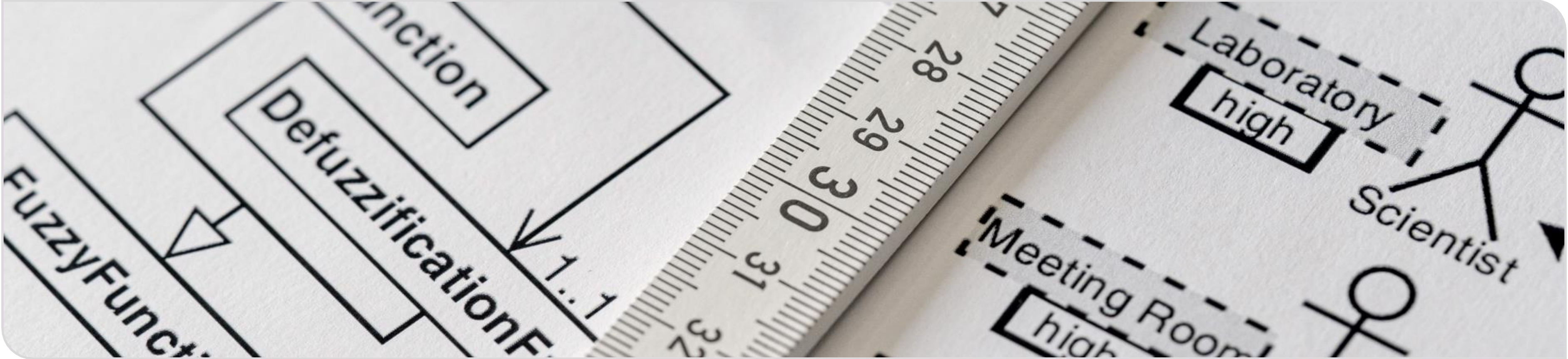
FluidTrust
Trust by fluid access control in Industry 4.0

DSiS
Dependability of Software-intensive Systems

Handling Environmental Uncertainty in Design Time Access Control Analysis

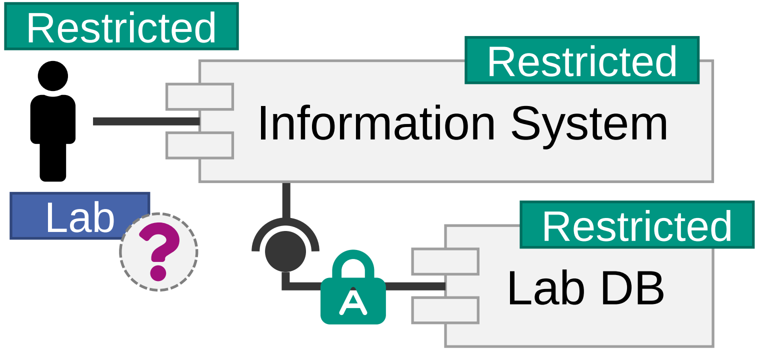
@ Euromicro Conference on Software Engineering and Advanced Applications, SEAA'22

**Nicolas Boltz, Sebastian Hahner, Maximilian Walter, Stephan Seifermann,
Petr Hnětynka, Tomáš Bureš, Robert Heinrich**

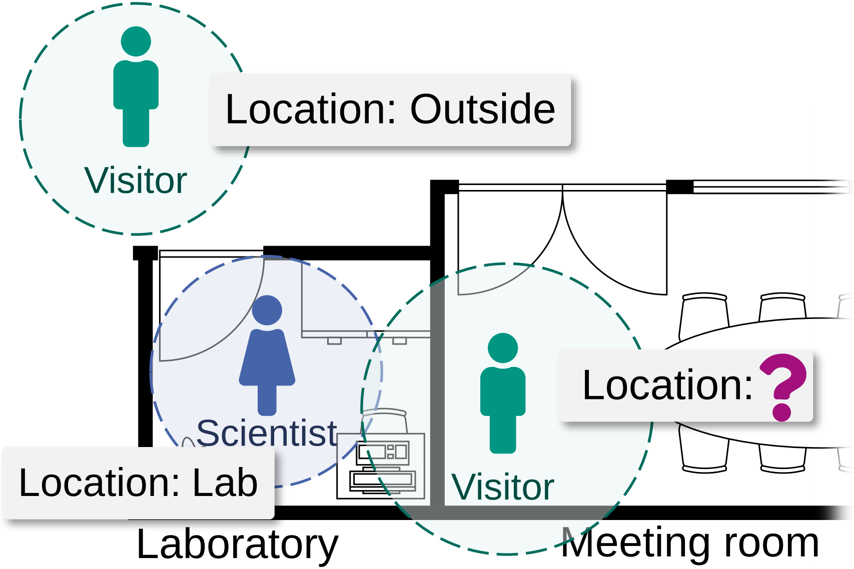


Design-Time Access Control Analysis

Data flow-based design-time analyses identify access control violations in architectural models **[1]**



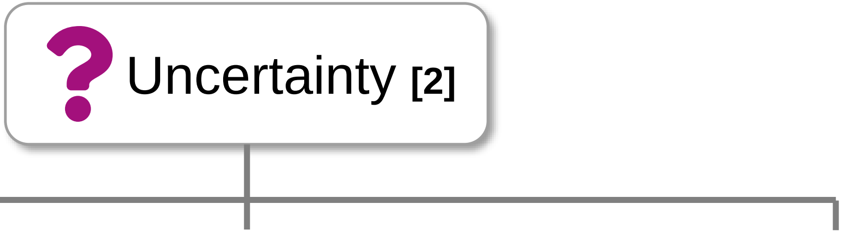
Policy: Restricted → Lab



Gap: Environmental uncertainty is ignored in data flow-based analyses!

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

Foundations: Classifying Uncertainty



Uncertainty [2]

Location

- **Context**: Completeness, w.r.t. the real world
- **Structural**: Accurately representing a subset of the real world
- **Input**: Values of parameters in use

Level

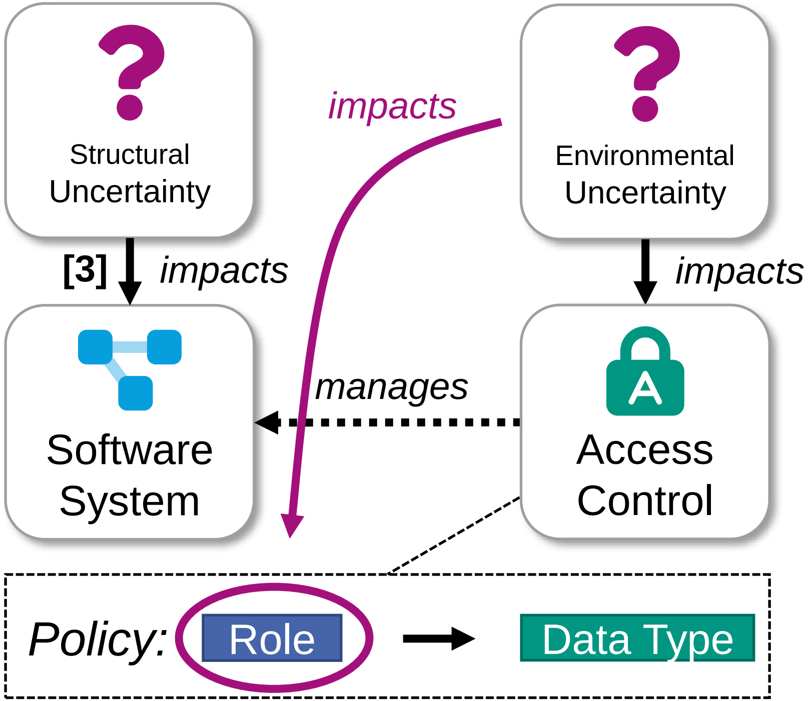
- **0**: Lack of uncertainty
- **1**: Lack of knowledge (i.e., *known unknowns*)
- **2**: Lack of awareness
- **3**: Lack of awareness and process
- **4**: Meta-uncertainty

Nature

- **Epistemic**: Lack of data, imperfection, lack of knowledge
- **Aleatory**: Inherent variability or random events

[2] D. Perez-Palacin and R. Mirandola, “Uncertainties in the modeling of self-adaptive systems: a taxonomy and an example of availability evaluation”, In: *ICPE*, 2014.

Handling Environmental Uncertainty



Research Question

How to analyze access control under environmental uncertainty at design time?

Contributions

- Notion of confidence to express the impact of environmental uncertainty
- Adapt existing data flow analysis **[1]**

Benefit

More *precise* and more *comprehensive* statements on a system's confidentiality

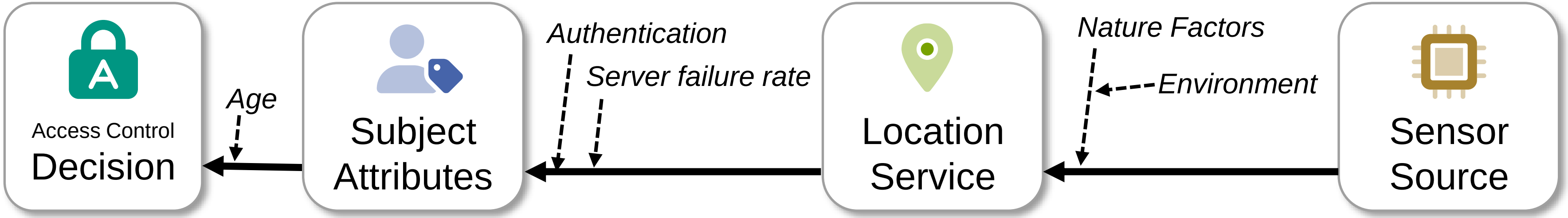
[1] S. Seifermann et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: *JSS*, vol. 184, 2022.
[3] M. Walter et al., "Architectural Optimization for Confidentiality under Structural Uncertainty", In: *ECSA-PP*, 2022.

Defining Confidence for Access Control

- **Confidence***:* Single value describing the validity of access control attributes
  - Trust Chains: Describes the trust in decision-influencing factors **[4]**
  - Include environmental factors in the modeling and analysis **[5]**
  - Describe the impact of known uncertainty

Factors

- Source of the information e.g., sensor type, physical access control
- Natural Factors impacting the accuracy, e.g., sensor noise, weather
- Age degrading the validity, e.g., measurement timing, processing delay

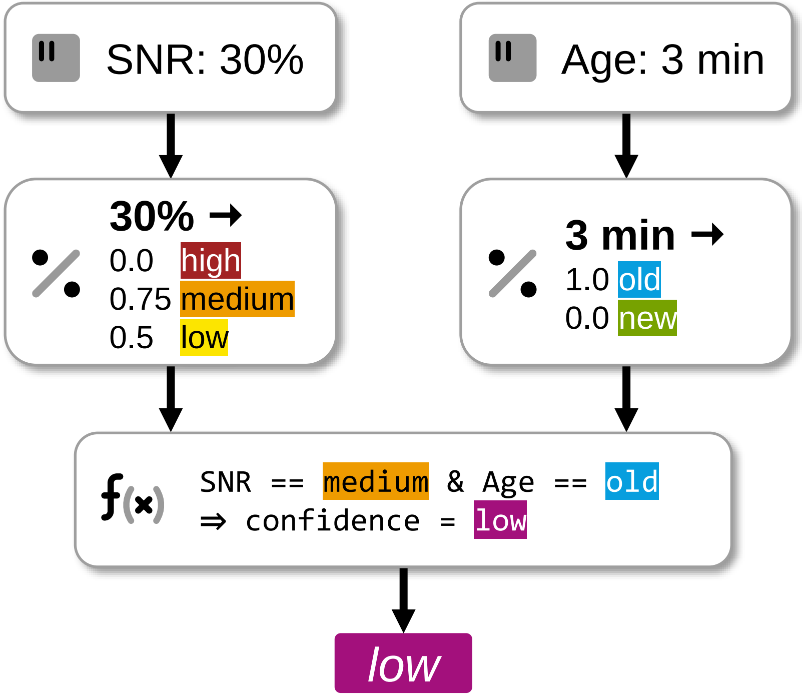


[4] V. Hu et al. “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, In: *NIST Special Publication 800.162*, 2014.
[5] U. Hengartner and G. Zhong. “Distributed, Uncertainty-Aware Access Control for Pervasive Computing”, In: *PerComW*, 2007.

Calculating Confidence from Influencing Factors

Use Fuzzy Inference Systems [6]

- Represent environmental factors as fuzzy values
- Define membership functions that use linguistic values
- Define rules that combine those values by using fuzzy inference
- Defuzzify the aggregated output to a confidence value



SNR: 30%

Age: 3 min

30% →
0.0 high
0.75 medium
0.5 low

3 min →
1.0 old
0.0 new

```
SNR == medium & Age == old
⇒ confidence = low
```

low

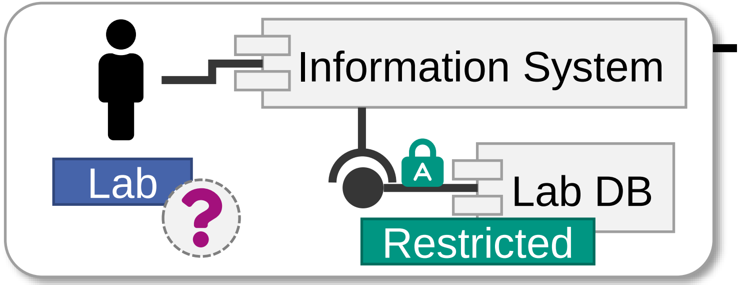
[6] G. Klir and B. Yuan. Fuzzy sets and fuzzy logic. Vol. 4. Prentice hall, New Jersey, 1995.

Including Confidence in Data Flow Analysis

Calculated Confidence:

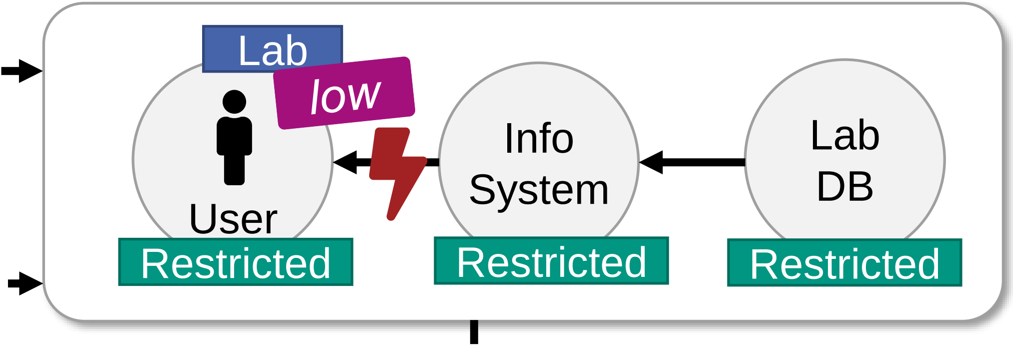
```
SNR == medium & Age == old
⇒ confidence = low
```

Software Architecture:



Policy: Restricted → Lab *high*

Data Flow Analysis [1]:



Using Prolog:

```
constraint_AccessControl (...) :-
char(‘Location’, SUBJ_LOC,
SUBJ_CONFIDENCE), \+ char(ST,
'Read Access', SUBJ_LOC, SUBJ_
CONFIDENCE), inputPin(PIN),
flowTree(PIN,S).
```

☒ Violation found!

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

Case Study-based Evaluation

Goal Question Metric Plan [7]

- Applicability: Expressiveness and availability of environmental factors
- Accuracy: Analyzing attribute-based violations, confidence-based, combinations

Case Study

- Reusing existing scenarios **[1]** with different access control, e.g., RBAC, or ABAC
- Use uncertainty-afflicted data to describe role and location, e.g., IP-address-based

Results

- Early definition and iterative refinement with more precise data is feasible
- *Default* confidence is transparent, no false-positives due to our extension
- High accuracy using confidence based on environmental factors

[1] S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
[7] V. Basili and D. Weiss. “A methodology for collecting valid software engineering data”, In: *TSE* 6, 1984.

Related Work

Uncertainty in Design Time Analysis

- Surveys on uncertainty **[8, 9, 10]**
- Design space exploration, e.g., using fuzzy logic **[11]** or quality prediction **[3]**
- *Gap: Focus on structural uncertainty*

Uncertainty in Access Control

- Using fuzzy logic to represent security patterns **[12]** or risk **[13]**
- Also focus on known uncertainty **[14,15]**
- *Gap: Lack of design-time analyzability*

[3] M. Walter et al., “Architectural Optimization for Confidentiality under Structural Uncertainty”, In: *ECSA-PP*, 2022.
[8] J. Troya et al. “Uncertainty representation in software models: a survey”, In: *SoSyM* 20.4, 2021.
[9] D. Sobhy et al., “Evaluation of Software Architectures under Uncertainty: A Systematic Literature Review”, In: *TOSEM*, 2021.
[10] S. Mahdavi-Hezavehi et al., “Uncertainty in Self-Adaptive Systems: A Research Community Perspective”, In: *TAAS*, 2021.
[11] N. Esfahani et al., “GuideArch: Guiding the exploration of architectural solution space under uncertainty”, In: *ICSE*, 2013.
[12] H. Hosmer, “Using fuzzy logic to represent security policies in the multipolicy paradigm”, In: *SIGSAC* 10.4, 1992.
[13] P. Cheng et al., “Fuzzy Multi-Level Security: An experiment on quantified risk-adaptive access control”, In: *IEEE SP*, 2007.
[14] C. Ardagna et al., “Supporting location-based conditions in access control policies”, In: *ACM CCS,* 2006.
[15] F. Cuppens and A. Miege, “Modelling contexts in the Or-BAC model”, In: *ACSAC,* 2003.

Conclusion and Future Work

- Problem: Modeling and analyzing the impact of environmental uncertainty on access control and confidentiality at design time
- Contribution: Defining and considering confidence in data flow analysis
  - Using fuzzy inference to describe different influential, environmental factors
  - Use confidence to define and analyze more expressive access control policies
- Benefit: More *precise* and more *comprehensive* confidentiality statements

Future Work

- Include more uncertainty types in design-time confidentiality analysis
- Predict the impact of uncertainty on confidentiality based on architectural modeling

References

[1] S. Seifermann et al., “Detecting violations of access control and information flow policies in data flow diagrams”, In: *JSS*, vol. 184, 2022.
[2] D. Perez-Palacin and R. Mirandola, “Uncertainties in the modeling of self-adaptive systems: a taxonomy and an example of availability evaluation”, In: *ICPE*, 2014.
[3] M. Walter et al., “Architectural Optimization for Confidentiality under Structural Uncertainty”, In: *ECSA-PP*, 2022.
[4] V. Hu et al. “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, In: *NIST Special Publication 800.162*, 2014.
[5] U. Hengartner and G. Zhong. “Distributed, Uncertainty-Aware Access Control for Pervasive Computing”, In: *PerComW,* 2007.
[6] G. Klir and B. Yuan. Fuzzy sets and fuzzy logic. Vol. 4. Prentice hall, New Jersey, 1995.
[7] V. Basili and D. Weiss. “A methodology for collecting valid software engineering data”, In: *TSE* 6, 1984.
[8] J. Troya et al. “Uncertainty representation in software models: a survey”, In: *SoSyM* 20.4, 2021.
[9] D. Sobhy et al., “Evaluation of Software Architectures under Uncertainty: A Systematic Literature Review”, In: *TOSEM*, 2021.
[10] S. Mahdavi-Hezavehi et al., “Uncertainty in Self-Adaptive Systems: A Research Community Perspective”, In: *TAAS*, 2021.
[11] N. Esfahani et al., “GuideArch: Guiding the exploration of architectural solution space under uncertainty”, In: *ICSE*, 2013.
[12] H. Hosmer, “Using fuzzy logic to represent security policies in the multipolicy paradigm”, In: *SIGSAC* 10.4, 1992.
[13] P. Cheng et al., “Fuzzy Multi-Level Security: An experiment on quantified risk-adaptive access control”, In: *IEEE SP*, 2007.
[14] C. Ardagna et al., “Supporting location-based conditions in access control policies”, In: *ACM CCS,* 2006.
[15] F. Cuppens and A. Miege, “Modelling contexts in the Or-BAC model”, In: *ACSAC,* 2003.