Karlsruhe Institute of Technology

ANYMOS

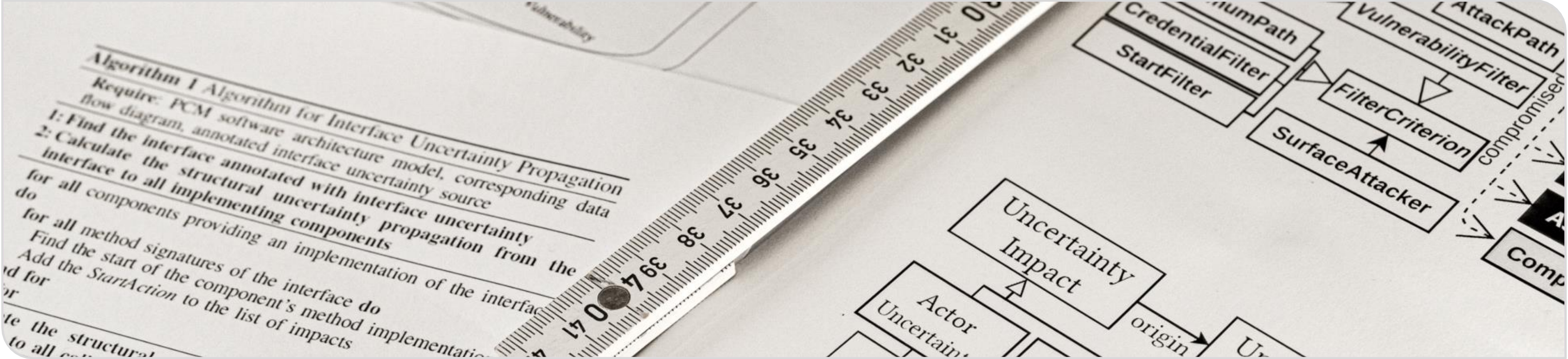
ANONYMISIERUNG FÜR VERNETZTE MOBILITÄTSSYSTEME

KASTEL

Architecture-based Propagation Analyses Regarding Security

GI Software Engineering 2024 – SE'24 – 29. February 2024

Sebastian Hahner, Maximilian Walter, Robert Heinrich, Ralf Reussner



Motivation

- Software security issues are wide-ranging [1] and increasingly common [2]
- Many issues can be detected by analyzing the software's architecture

Top 10:2021 List [1]

A01 Broken Access Control
A02 Cryptographic Failures
A03 Injection
A04 Insecure Design
A05 Security Misconfiguration
A06 Vulnerable and Outdated Components
A07 Identification and

OWASP®

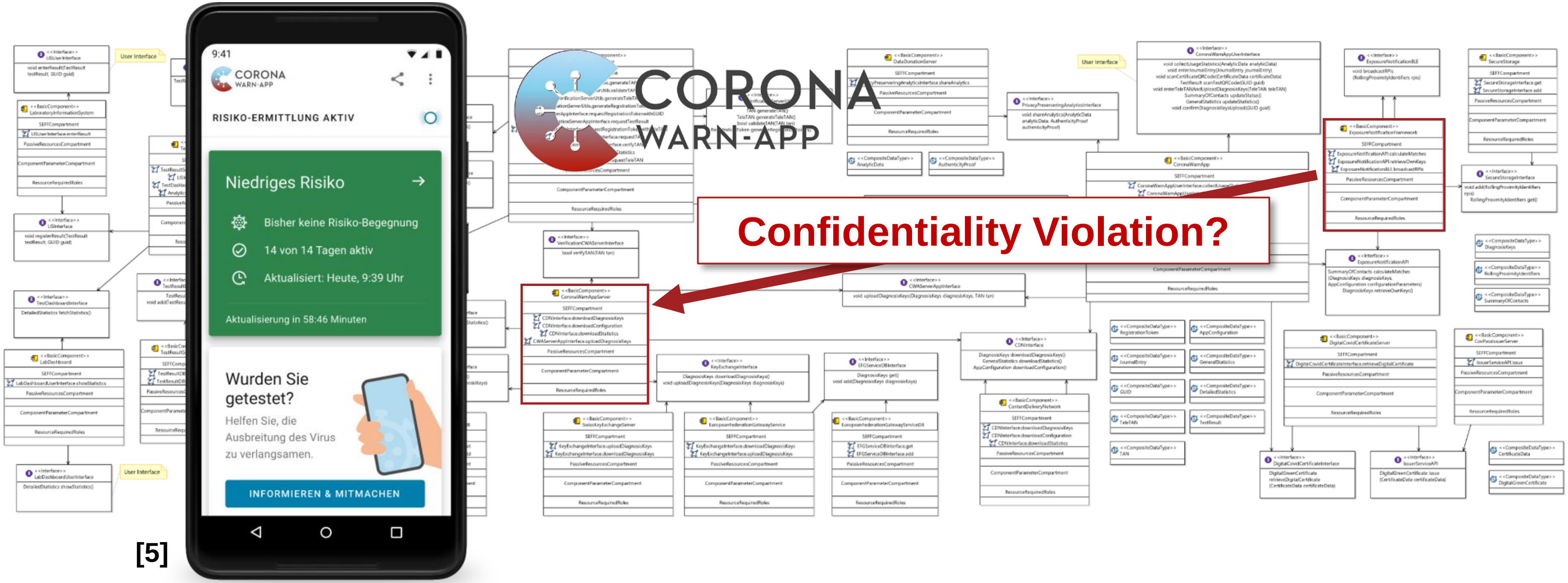
Examples

- Access control and vulnerability analysis [3]
- Attack path detection and propagation
- Data flow-based confidentiality analysis [4]
- Uncertainty propagation *w.r.t.* confidentiality

[1] OWASP, "Top Ten Web Application Security Risks", https://owasp.org/, 2021.
[2] UK Department for Digital, Culture, Media and Sport, "Cyber Security Breaches Survey", 2021.
[3] M. Walter, R. Heinrich, and R. Reussner, "Architectural Attack Propagation Analysis for Identifying Confidentiality Issues", In: *IEEE ICSA*, 2022.
[4] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: *JSS*, vol. 184, 2022.

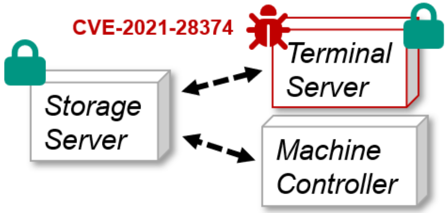
Karlsruhe Institute of Technology

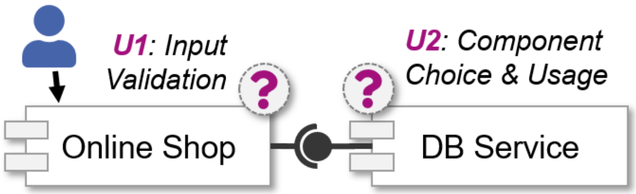
Motivation



[5] Robert Koch Institute, Open-source Corona Warn App, documentation available online: https://github.com/corona-warn-app

Overview





Attack Path Detection

- Generating attack paths from software architectural models, access control policies and known vulnerabilities
- Detecting and filtering attack paths

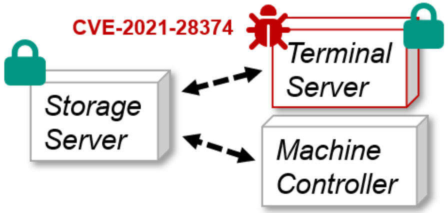
➪ *M. Walter et al., “Architecture-Based Attack Path Analysis for Identifying Potential Security Incidents”, ECSA, Springer, 2023.*

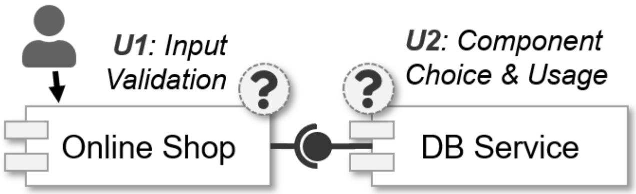
Uncertainty Impact Analysis

- Estimates the impact of uncertainty sources on a system’s confidentiality
- Architecture-based and data flow-based propagation of uncertainty

➪ *S. Hahner et al., “Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality”, SEAMS, IEEE/ACM, 2023.*

Overview





Attack Path Detection

- Generating attack paths from software architectural models, access control policies and known vulnerabilities
- Detecting and filtering attack paths

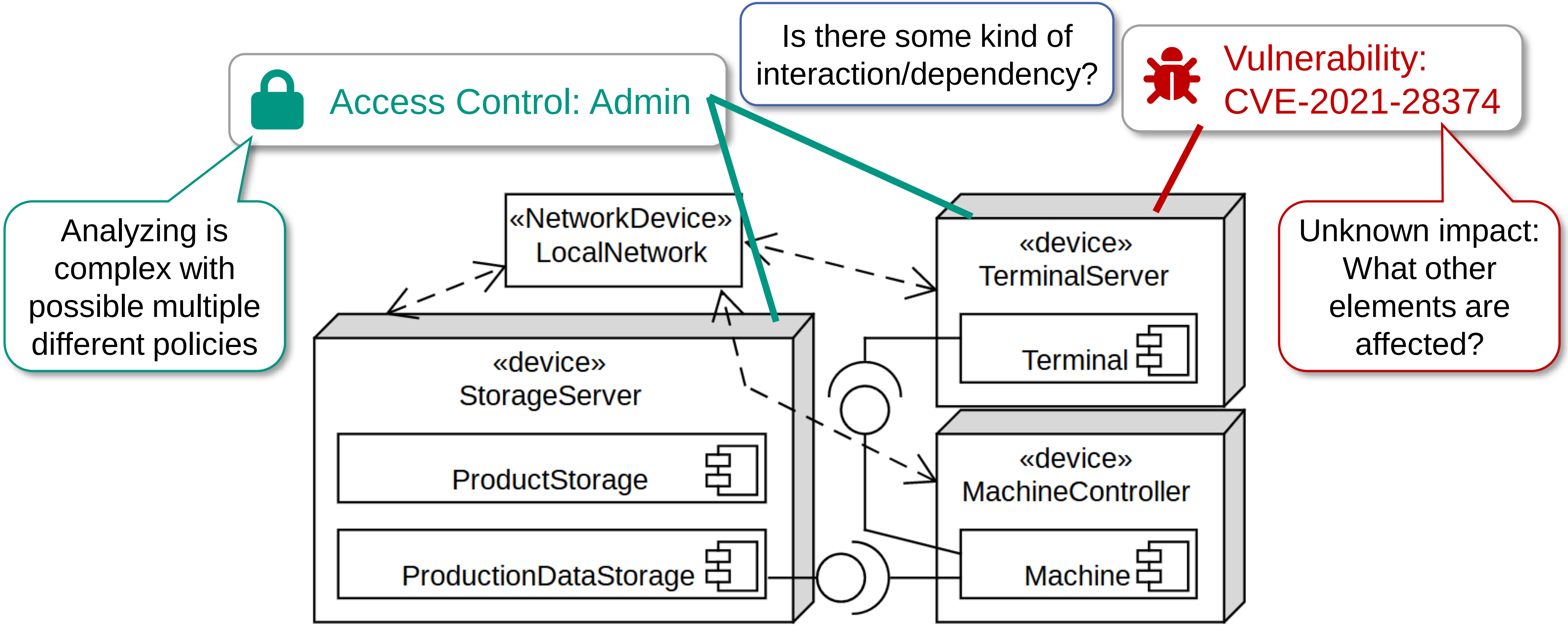
➪ *M. Walter et al., "Architecture-Based Attack Path Analysis for Identifying Potential Security Incidents", ECSA, Springer, 2023.*

Uncertainty Impact Analysis

- ❑ Estimates the impact of uncertainty sources on a system's confidentiality
- ❑ Architecture-based and data flow-based propagation of uncertainty

➪ *S. Hahner et al., "Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality", SEAMS, IEEE/ACM, 2023.*

Attack Path Detection – Motivation



Modeling of Access Control and Vulnerabilities

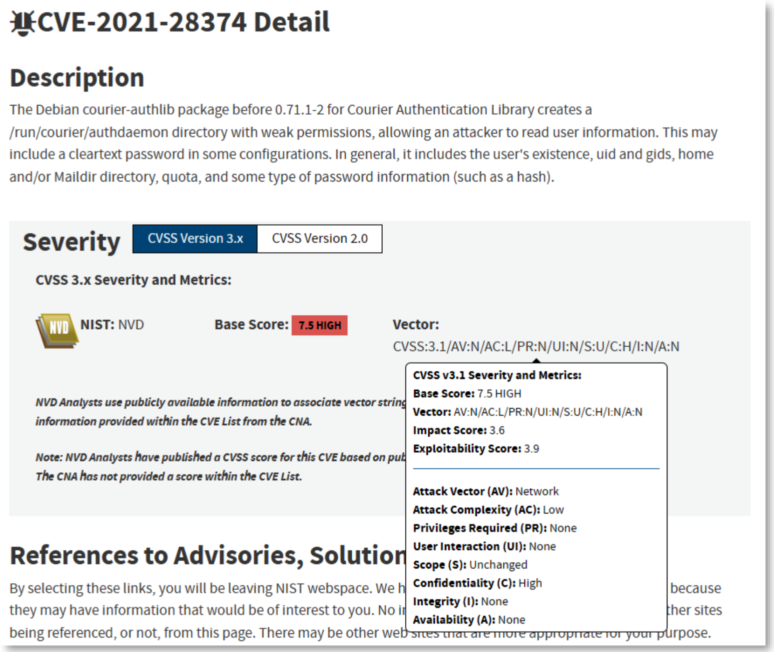
Karlsruhe Institute of Technology

Access Control

- Based on the XACML [6]
- OASIS industry standard for attribute-based access control
- Benefits: Well-known and documented

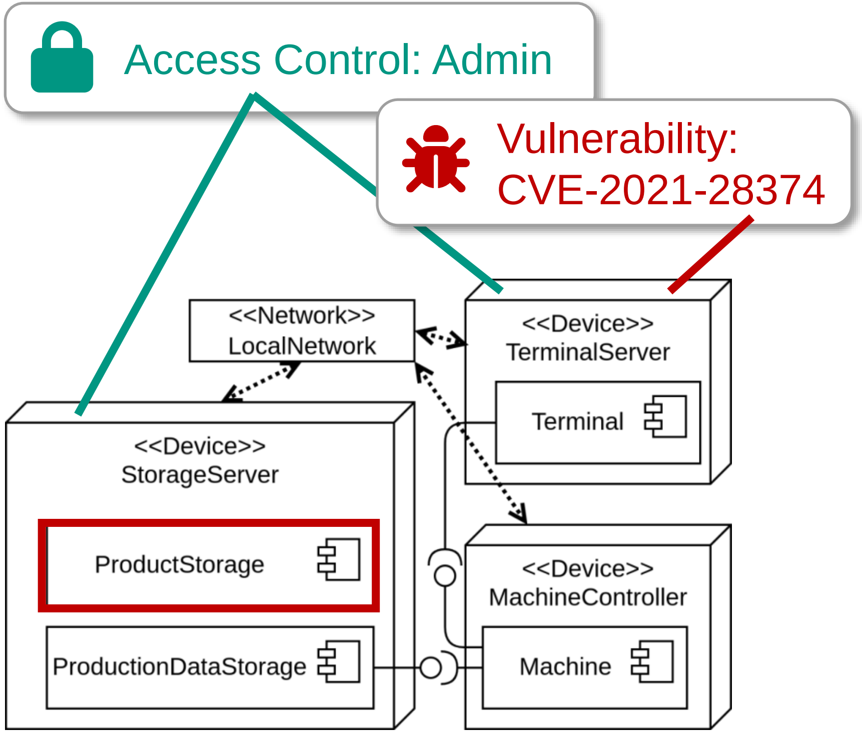
Vulnerabilities

- Reuse existing classification of vulnerabilities and their impact [7]
- Adapt attacker capabilities, e.g., gained access control attributes



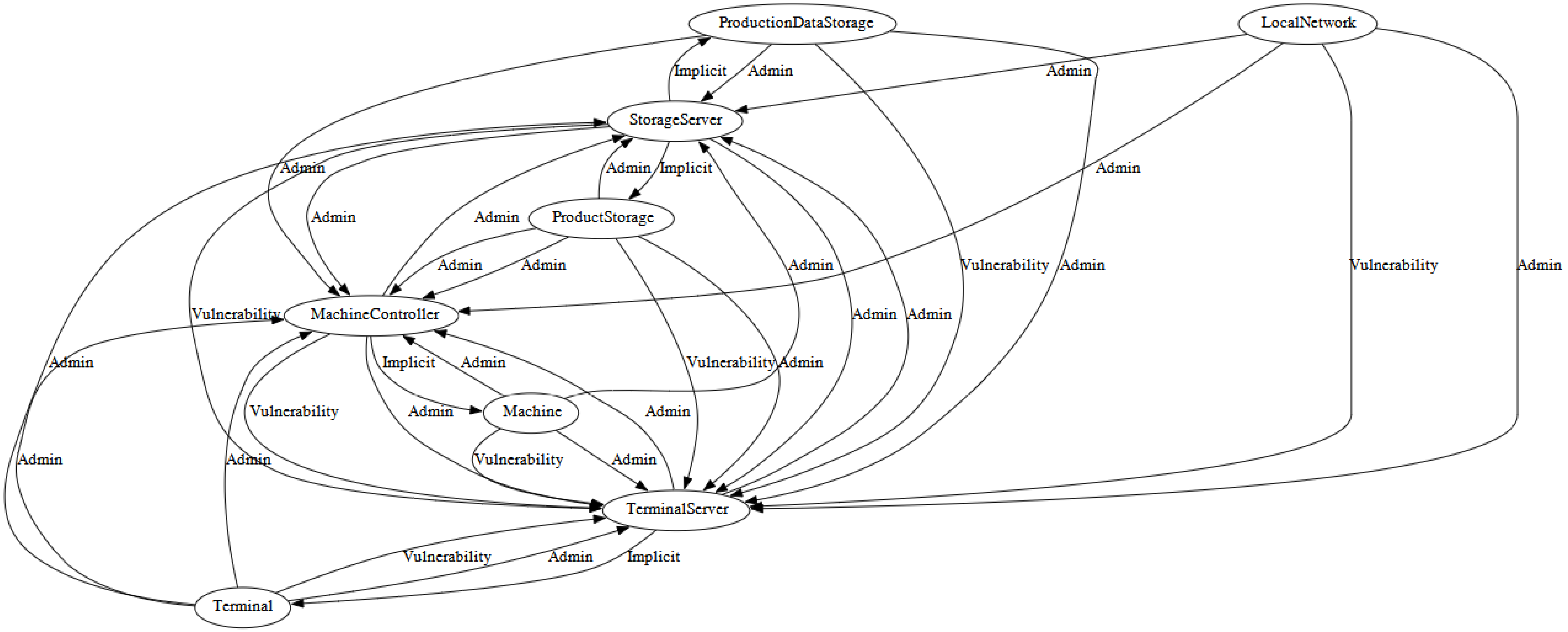
[6] OASIS, “eXtensible Access Control Markup Language (XACML)”, see: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
[7] „Common Vulnerabilities and Exposures“ and „Common Weakness Enumeration“, see: https://www.cve.org/ or https://nvd.nist.gov/

Attack Path Creation

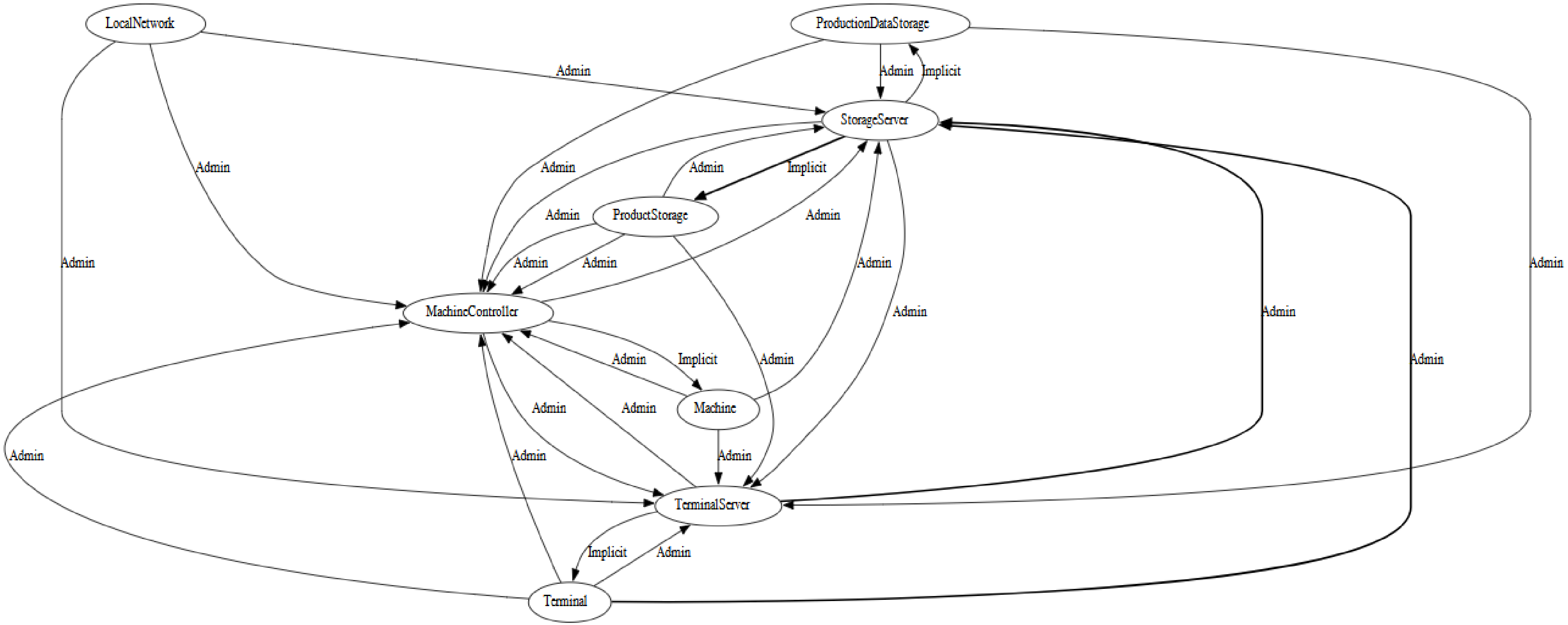


- Create multi label graph, derived from the software architecture
- Nodes are architectural elements
- Edges are possibilities to compromise
- Use Filters to remove edges, e.g.,
  - Specific vulnerabilities
  - Start element
  - Maximum path length
  - Attacker capabilities
  - Initial credentials

Attack Graph – Without Filter

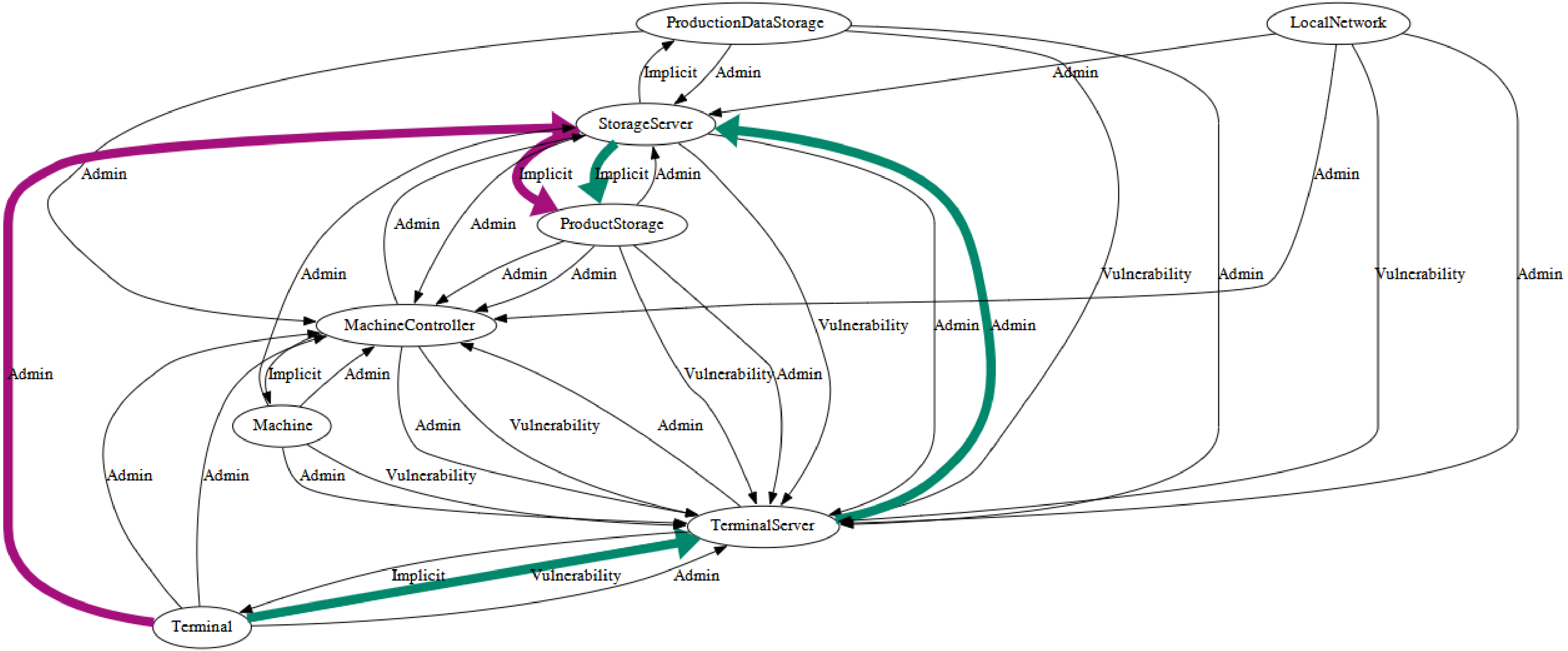


Attack Graph – With Vulnerability Filter



Karlsruhe Institute of Technology

Attack Path Identification



Accuracy Evaluation

Design

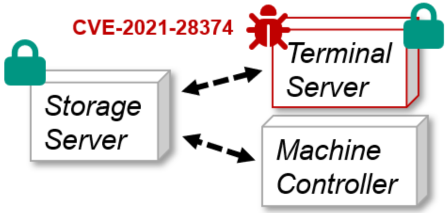
- Goal: Investigate how well attack path identifications works
- 5 scenarios with 52 attack paths, including real-world breaches and evaluation cases
- Metrics: Precision, Recall, F1-score

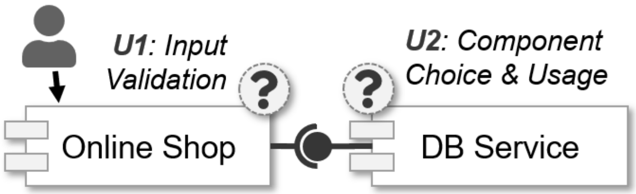
Results

- High identification rate
- Missing attack paths due to trade-off between accuracy/scalability

Case	Precision	Recall	F1-score
Target	1.00	1.00	1.00
Power Grid	1.00	0.88	0.93
Cloud Storage	1.00	1.00	1.00
Travel Planner	1.00	1.00	1.00
Maintenance	1.00	0.86	0.92

Overview





Attack Path Detection

- Generating attack paths from software architectural models, access control policies and known vulnerabilities
- Detecting and filtering attack paths

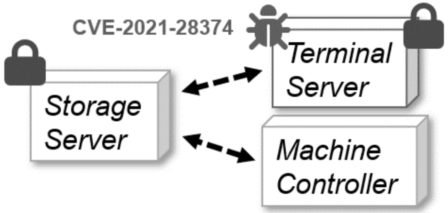
➪ *M. Walter et al., "Architecture-Based Attack Path Analysis for Identifying Potential Security Incidents", ECSA, Springer, 2023.*

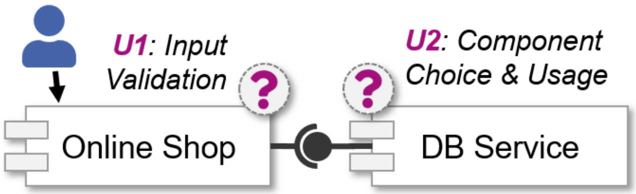
Uncertainty Impact Analysis

- ❑ Estimates the impact of uncertainty sources on a system's confidentiality
- ❑ Architecture-based and data flow-based propagation of uncertainty

➪ *S. Hahner et al., "Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality", SEAMS, IEEE/ACM, 2023.*

Overview





Attack Path Detection

- Generating attack paths from software architectural models, access control policies and known vulnerabilities
- Detecting and filtering attack paths

➪ *M. Walter et al., "Architecture-Based Attack Path Analysis for Identifying Potential Security Incidents", ECSA, Springer, 2023.*

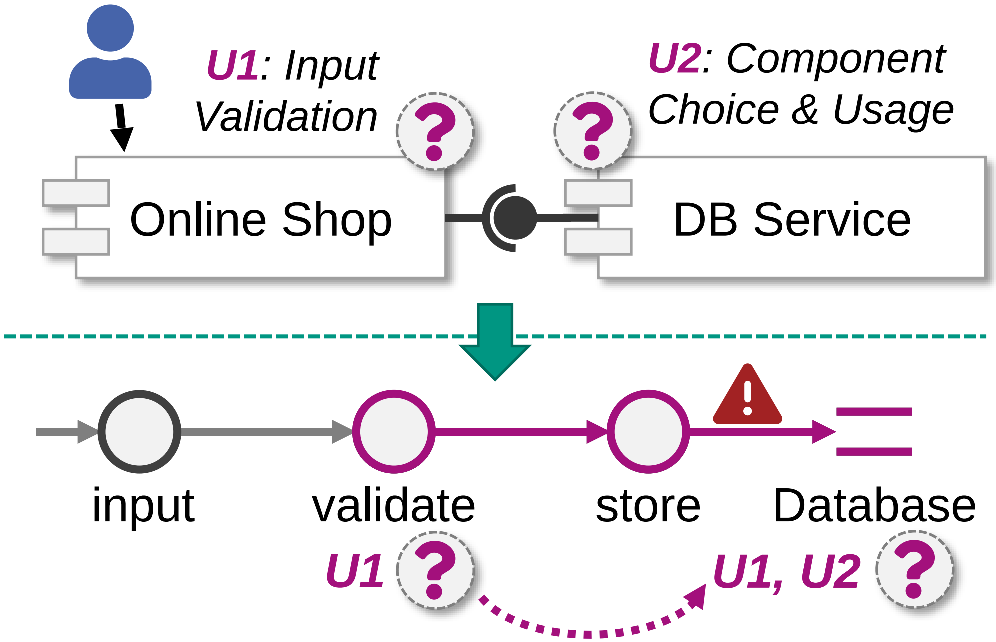
Uncertainty Impact Analysis

- Estimates the impact of uncertainty sources on a system's confidentiality
- Architecture-based and data flow-based propagation of uncertainty

➪ *S. Hahner et al., "Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality", SEAMS, IEEE/ACM, 2023.*

Uncertainty Impact Analysis – Motivation

- Uncertainty has an impact on a software system's confidentiality
  - Uncertainty sources exist in the system and its environment **[8]**
  - Design time analysis can find confidentiality violations **[9, 10]**



Challenges

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

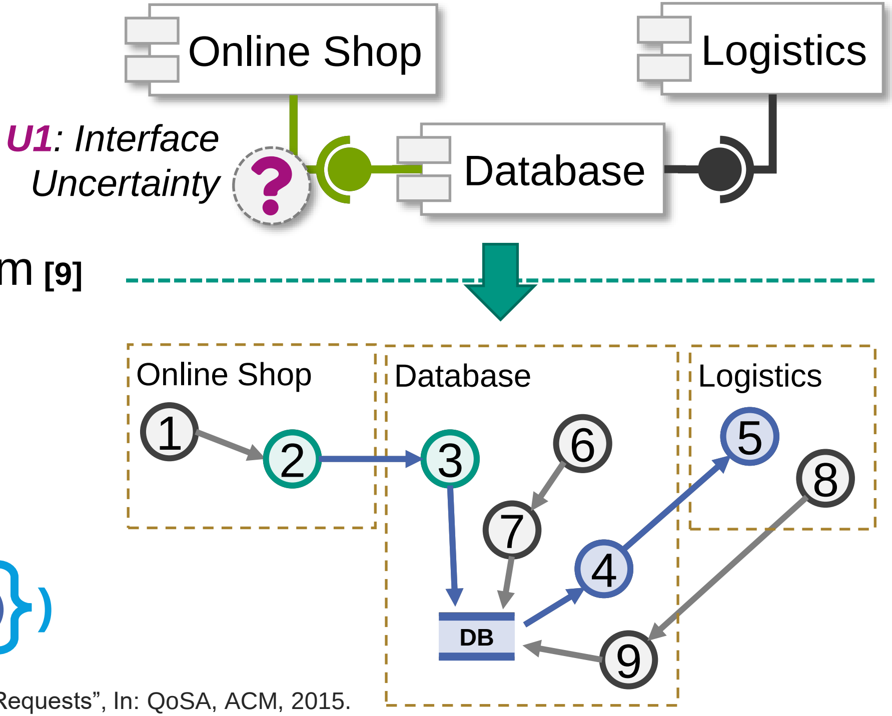
[8] M. Acosta et al., „Uncertainty in coupled models of cyber-physical systems", In: MODELS-C, ACM, 2022.
[9] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: *JSS*, vol. 184, 2022.
[10] S. Hahner, et al., "Model-based Confidentiality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

Uncertainty Impact Analysis on Confidentiality

Impact Analysis Algorithm

1) Annotate the uncertainty source
2) Calculate structural propagation based on change impact analysis **[11]**
3) Map all impacts to the data flow diagram **[9]**
4) Calculate the propagation along all affected data flows
5) Calculate the impact set by finding the maximum discontiguous data flows

$max_D(\{2\ 3\ \text{DB}\ 4\ 5\}, \{3\ \text{DB}\ 4\ 5\})$

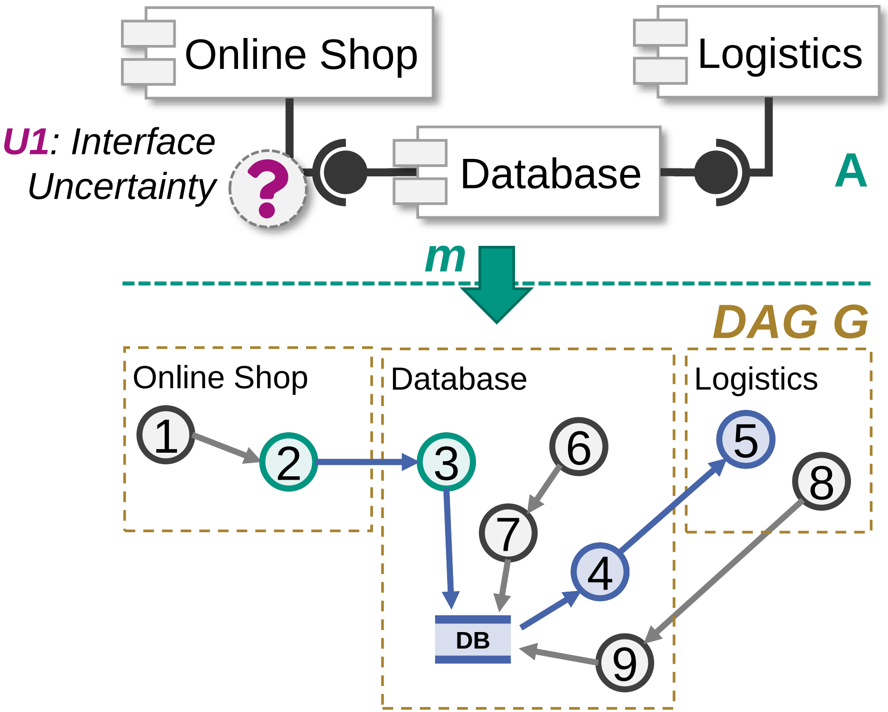


[11] K. Rostami, et al., "Architecture-based Assessment and Planning of Change Requests", In: QoSA, ACM, 2015.
[9] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: JSS, vol. 184, 2022.

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: $\forall\, x \in X \subseteq V, \exists\, a \in A : m(a) \prec x$



Case Study-based Evaluation

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 **[9]**

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

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

Karlsruhe Institute of Technology

Related Work

Attack Path Detection

- Policy analysis [12], model-driven confidentiality analysis [9, 13], and attacker modelling and analysis [14]

⇨ *Related approaches lack either fine-grained policy or attack models*

Uncertainty Impact Analysis

- Architecture-based uncertainty analyses [15, 16, 17], and uncertainty-aware confidentiality analysis [18]

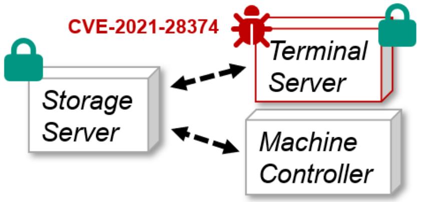
⇨ *Related approaches lack either precision or comprehensiveness*

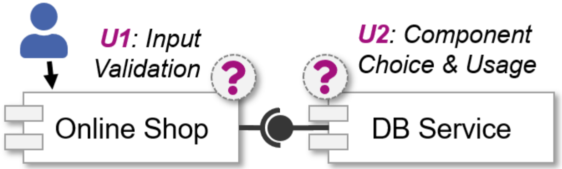
[9] S. Seifermann, et al., "Detecting violations of access control and information flow policies in data flow diagrams", In: JSS, vol. 184, 2022.
[12] K. Fisler, et al., "Verification and change-impact analysis of access-control policies", In: ICSE, IEEE, 2005.
[13] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development", In: UML, Springer 2002.
[14] M. Aksu, "Automated Generation of Attack Graphs Using NVD", In: CODASPY, ACM, 2018.
[15] N. Esfahani, et al., "GuideArch: Guiding the exploration of architectural solution space under uncertainty", In: ICSE, IEEE, 2013.
[16] I. Lytra and U. Zdun, "Supporting architectural decision making for systems-of-systems design under uncertainty", In: SESoS, ACM, 2013.
[17] A. Koziolek, et al., "PerOpteryx: Automated application of tactics in multi-objective software architecture optimization", In: QoSA-ISARCS, ACM, 2011.
[18] N. Boltz, et al., "Handling environmental uncertainty in design time access control analysis", In: *SEAA*, IEEE, 2022.

Conclusion

- Software architecture-based analyses can help in identifying security issues
- These analyses propagate information on intermediate representations like attack graphs or data flow diagrams

- **Attack Path Detection** [A] generates attack paths to analyze vulnerabilities
- **Uncertainty Impact Analysis** [B] propagates uncertainty to predict its impact on the system's confidentiality





Contact

What's next?

Uncertainty Flow Diagrams [19], using uncertainty propagation for interactions

[A] M. Walter, R. Heinrich, and R. Reussner, "Architecture-Based Attack Path Analysis for Identifying Potential Security Incidents", In: ECSA, Springer, 2023.
[B] S. Hahner, R. Heinrich, and R. Reussner, "Architecture-Based Uncertainty Impact Analysis to Ensure Confidentiality", In: SEAMS, IEEE/ACM, 2023.
[19] J. Cámara, S. Hahner, D. Perez-Palacin, A. Vallecillo, M. Acosta, N. Bencomo, R. Calinescu, S. Gerasimou, "Uncertainty Flow Diagrams: Towards a Systematic Representation of Uncertainty Propagation and Interaction in Adaptive Systems", In: SEAMS, IEEE/ACM, 2024, accepted, to appear.