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]

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

Foundations: Classifying Uncertainty

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

---

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

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

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

Including Confidence in Data Flow Analysis

Calculated Confidence:

\[ f(x) \text{ SNR} = \text{medium} \& \text{Age} = \text{old} \Rightarrow \text{confidence} = \text{low} \]

Software Architecture:

Data Flow Analysis [1]:

Using Prolog:

```prolog
constraint_AccessControl (...) :-
  char('Location', SUBJ_LOC, SUBJ_CONFIDENCE), \
  char(ST, 'Read Access', SUBJ_LOC, SUBJ_CONFIDENCE), \
  inputPin(PIN), \
  flowTree(PIN,S).
```

Violation found!

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

Related Work

Uncertainty in Design Time Analysis
- Surveys on uncertainty [8, 9, 10]
- 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

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