Model-based Confidentiality Analysis under Uncertainty

3rd International Workshop on Model-driven Engineering for Software Architecture, MDE4SA 2023
20th IEEE International Conference on Software Architecture, ICSA 2023

Sebastian Hahner, Tizian Bitschi, Maximilian Walter, Tomáš Bureš, Petr Hnětynka, Robert Heinrich
Motivation

- Data flow-based design-time analyses identify confidentiality violations in architectural models [1]
  - Model software architecture
  - Define characteristics and constraints
  - Analyze data flows on confidentiality

- Challenge: Uncertainty both in the system and its environment [2]
- Gap: Existing approaches use the modeled information suboptimally

---


Overview

Idea: Extend an existing data flow-based confidentiality analysis [1]
- Reuse existing modeling techniques
- Trace annotated uncertainty

Contributions
- Discussion of available information at design time and how to use it
- An uncertainty-aware confidentiality analysis based on model variation

Expressing Uncertainty as Model Variation

Uncertainty: “any departure from the unachievable ideal of complete determinism” [3]

- Design uncertainty is “normally represented in software models by variability models” [4]
- Variation model represents all known uncertainty impacts
- Variant Generation creates all possible variants of the software architecture [5]
- Usable with existing analyses

Available Information in Modeling and Analysis

Confidentiality
- Violation occurrence
- Violated constraint
- Location in the model
- Variable state

Uncertainty
- Source
- Classification
- Impact in the model
- Mitigation
- Uncertainty Interaction
Towards Uncertainty Awareness

Naive approach
- Rejects the complete architecture
- Uses the violation occurrence only

Scenario-aware
- Only rejects variants with violations
- Uses uncertainty impact and violation occurrence

Data flow-aware
- Traces violations back to potentially causing uncertainty impacts
- Yields affected data flows

**U1: Data Encryption**
- Product DB
- Shop
- User DB

**U2: User DB Allocation**
- Cloud
- On Premise

**U3: Product DB Allocation**
- On Premise
- Cloud
Uncertainty-Aware Confidentiality Analysis

**Constraint:** Personal $\rightarrow$ Cloud

**Variant Generation**

**Variation model:**

A: On Premise

B: Cloud

**Data flow-based Analysis**

- Personal User
  - Shop
  - DB
  - Cloud

- Personal User
  - Shop
  - DB
  - Cloud

Introduction ▶ Foundations ▶ Contributions ▶ Evaluation ▶ Related Work ▶ Conclusion
Uncertainty-Aware Confidentiality Analysis

**Constraint:** 

- Personal
- Cloud

**Variation model:**

- A: On Premise
- B: Cloud

**Data flow-based Analysis**

- Personal
- User
- Shop
- Cloud
- DB
- ¬Cloud

**Variant Generation**

- Shop
- DB
- User
- Shop
- DB
- User
There are 4 variants with confidentiality violations. All violations happen in the User DB. This is due to uncertainties: U1, U2. Product DB and U3 are not involved.
Case Study-based Evaluation

Goal Question Metric Plan [6]

- **Accuracy**: Measure precision and recall regarding uncertainty, compare with SOTA
- **Usability**: Reducing effort and complexity for software architects at design time

Case Study

- Reusing existing scenarios [1] with different confidentiality requirements
- Apply the naive approach, the scenario-aware and the data flow-aware approach

Results

- Expected: All approaches have a high recall, but the precision differs
- The data flow-aware approach correctly identifies relevant uncertainty impacts
- Effort reduction compared to manual analysis only using design time information

---


Related Work

- Pattern-based [7] or data flow-based analysis [1]
  - No uncertainty

- Design space exploration like GuideArch [8] or PerOpteryx [9]
  - No confidentiality

Our approach

- Design-time confidentiality analysis
- Architecture-based uncertainty analysis

Uncertainty-aware confidentiality analysis is only scenario-aware

- Combination of data flow-based analysis with PerOpteryx [10]

---

Conclusion

- **Problem:** Analyzing confidentiality while considering uncertainty at design time
- **Contribution:** Uncertainty-aware confidentiality analysis based on model variation
- **Benefit:** Precise confidentiality statements considering data flows and uncertainty

Future Work

- Connect confidentiality analysis to Uncertainty Impact Analysis [12]
- Move variant generation in the data flow analysis
- Support more uncertainty types beyond scenario uncertainty

References