Architecture-based Propagation Analyses Regarding Security

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.

Examples

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

Introduction ▶️ Attack Path Detection ▶️ Uncertainty Impact Analysis ▶️ Related Work ▶️ Conclusion
Motivation

Confidentiality Violation?

Overview

Introduction ▶ Attack Path Detection ▶ Uncertainty Impact Analysis ▶ Related Work ▶ Conclusion

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


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

Overview

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

Uncertainty Impact Analysis
- Estimates the impact of uncertainty sources on a system’s confidentiality
- Architecture-based and data flow-based propagation of uncertainty
Introduction ▶ Attack Path Detection ▶ Uncertainty Impact Analysis ▶ Related Work ▶ Conclusion

Attack Path Detection – Motivation

Access Control: Admin

- Analyzing is complex with possible multiple different policies
- Vulnerability: CVE-2021-28374
- Unknown impact: What other elements are affected?

Is there some kind of interaction/dependency?

Analyzing is complex with possible multiple different policies

Access Control: Admin

- Vulnerability: CVE-2021-28374
- Unknown impact: What other elements are affected?

Is there some kind of interaction/dependency?
Modeling of Access Control and Vulnerabilities

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

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

Introduction ▶ Attack Path Detection ▶ Uncertainty Impact Analysis ▶ Related Work ▶ Conclusion
Introduction ▶ Attack Path Detection ▶ Uncertainty Impact Analysis ▶ Related Work ▶ Conclusion

Attack Graph – With Vulnerability Filter
Attack Path Identification

Introduction ▶ Attack Path Detection ▶ Uncertainty Impact Analysis ▶ Related Work ▶ Conclusion

S. Hahner, M. Walter, R. Heinrich, R. Reussner – Architecture-based Propagation Analyses Regarding Security

KASTEL – Institute of Information Security and Dependability
DSIS – Dependability of Software-intensive Systems group
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

<table>
<thead>
<tr>
<th>Case</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Power Grid</td>
<td>1.00</td>
<td>0.88</td>
<td>0.93</td>
</tr>
<tr>
<td>Cloud Storage</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Travel Planner</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Maintenance</td>
<td>1.00</td>
<td>0.86</td>
<td>0.92</td>
</tr>
</tbody>
</table>
Overview

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

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

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

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

---

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

\[ \max_D \{ \{2, 3, DB, 4, 5\}, \{3, DB, 4, 5\} \} \]

Uncertainty Impact Analysis on Confidentiality

Formal Foundation of Impact Analysis

- Data flow diagrams can be represented as $\text{DAG } G = (V, E)$ with a strict partial order $u < v$

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

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

<table>
<thead>
<tr>
<th></th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
<th>AVG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Precision P</strong></td>
<td>0.838</td>
<td>1.000</td>
<td>0.840</td>
<td>0.882</td>
<td>0.890</td>
</tr>
<tr>
<td><strong>Recall R</strong></td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
<td>1.000</td>
</tr>
<tr>
<td>( F_1 ) score</td>
<td>0.912</td>
<td>1.000</td>
<td>0.913</td>
<td>0.938</td>
<td>0.942</td>
</tr>
<tr>
<td>( r_a )</td>
<td>0.155</td>
<td>0.080</td>
<td>0.105</td>
<td>0.300</td>
<td>0.160</td>
</tr>
<tr>
<td>( r_i )</td>
<td>0.185</td>
<td>0.080</td>
<td>0.125</td>
<td>0.340</td>
<td>0.183</td>
</tr>
</tbody>
</table>

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

---

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

What’s next?
Uncertainty Flow Diagrams [19], using uncertainty propagation for interactions

---