R. Rabiser, M. Wimmer, I. Groher, A. Wortmann, B. Wiesmayr (Hrsg.): SE 2024,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2024 121

Architecture-based Propagation Analyses Regarding Security

Sebastian Hahner[1] Maximilian Walter[2] Robert Heinrich[3] Ralf Reussner[4]

Keywords: Software Architecture; Propagation; Security; Confidentiality; Uncertainty

1 Introduction and Overview

In our modern world, the ever-expanding exchange of data and the increased complexity of interconnected software systems make software security challenging. Ideally, security concerns are already addressed early, as discussed with *security by design*. Here, architecture-based modeling enables the analysis of security threats such as confidentiality violations or targeted attacks. Such analyses leverage the structural properties of software architecture and information about the system context like deployment and usage [Re16]. However, this requires security-specific model annotations and adapted propagation rules. In this paper, we present two architectural propagation analyses [HHR23; WHR23b] that extend the concept of change impact analysis [He18] for security analysis. Both analyses build on the architecture modeling language PCM [Re16]. The former propagates uncertainty in software architectures and predicts its impact on the system's confidentiality. The latter identifies attack paths using vulnerabilities and access control properties in attacker propagation.

2 Uncertainty Impact Analysis

Our uncertainty impact analysis [HHR23] enables the early detection and mitigation of confidentiality violations due to uncertainty. This is achieved by combining the structural propagation using the software architecture model with data flow-based propagation of uncertainty. Different types of uncertainty sources [Ha23] like *behavior uncertainty* and *connector uncertainty* can be annotated and propagated using propagation rules adapted from change impact analysis [He18]. Afterward, we automatically extract all potential data flows and trace the impact of uncertainty within these flows to predict confidentiality violations. The calculated impact set helps in what-if scenarios without laborious modeling and analysis of confidentiality. We evaluated the approach on four evaluation scenarios with a total of 19 components and 200 data flow diagram nodes. The accuracy evaluation shows a high F1-score of 0.94 while reducing the effort compared to a manual analysis by 82%.

[1] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, sebastian.hahner@kit.edu
[2] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, maximilian.walter@kit.edu
[3] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, robert.heinrich@kit.edu
[4] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, ralf.reussner@kit.edu

doi:10.18420/sw2024_38

3 Attack Path Detection

Our attack path detection approach [WHR23b] uses software architecture models to detect potential attack paths leading to a targeted element. The security properties within the software architecture are described using an access control and vulnerability meta model [Wa23; WHR23a]. Our approach first creates an attack graph for the software architecture. This graph contains the vulnerabilities and access control policies and shows how attackers can compromise elements in the system. Afterward, our approach tries to identify for each element in the system a path to the targeted element. Software architects can specify filter criteria to remove irrelevant paths. We evaluated the approach on five evaluation scenarios with 52 attack paths regarding accuracy and scalability. The accuracy evaluation shows a high F1-score between 0.92 and 1.00 with a sufficient runtime.

4 Conclusion and Future Work

In this paper, we presented two security analysis approaches that use architecture-based propagation. In future work, we plan to research uncertainty propagation in confidentiality analysis for a broader range of uncertainty types and with increased precision. Furthermore, we aim to integrate the aforementioned approaches for comprehensive analysis results.

Acknowledgment: This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs and also by the German Federal Ministry of Education and Research (BMBF) grant number 16KISA086 (ANYMOS).

References

[Ha23] Hahner, S. et al.: A Classification of Software-Architectural Uncertainty Regarding Confidentiality. In: ICETE. 2023.

[He18] Heinrich, R. et al.: Architecture-based change impact analysis in cross-disciplinary automated production systems. JSS 146/1, 2018.

[HHR23] Hahner, S.; Heinrich, R.; Reussner, R.: Architecture-based Uncertainty Impact Analysis to ensure Confidentiality. In: SEAMS. IEEE/ACM, 2023.

[Re16] Reussner, R. et al.: Modeling and Simulating Software Architectures – The Palladio Approach. MIT Press, 2016.

[Wa23] Walter, M. et al.: Architecture-based attack propagation and variation analysis for identifying confidentiality issues in Industry 4.0. at - Automatisierungstechnik 71/6, 2023.

[WHR23a] Walter, M.; Heinrich, R.; Reussner, R.: Architectural Attack Propagation Analysis for Identifying Confidentiality Issues. In: ICSA. IEEE, 2023.

[WHR23b] Walter, M.; Heinrich, R.; Reussner, R.: Architecture-based Attack Path Analysis for Identifying Potential Security Incidents. In: ECSA. 2023.