# Dataset - Architectural Attack Propagation Analysis for Identifying Confidentiality Issues

Maximilian Walter
*Karlsruhe Institute of Technology (KIT)*
Karlsruhe, Germany
maximilian.walter@kit.edu

Robert Heinrich
*Karlsruhe Institute of Technology (KIT)*
Karlsruhe, Germany
robert.heinrich@kit.edu

Ralf Reussner
*Karlsruhe Institute of Technology (KIT)*
Karlsruhe, Germany
ralf.reussner@kit.edu

***Abstract*—Connecting different systems to exchange data increases the number of potential vulnerabilities. These vulnerabilities can be combined with access control issues and enables attacker to propagate through the system. We developed an attack propagation analysis for analysing this dependency between vulnerabilities and access control policies. This helps architects to estimate the confidentiality of the system. We provide the developed analysis, metamodels, and the evaluation data as a public dataset.**

***Index Terms*—Confidentiality, Attacker Propagation, Software Architecture, Dataset**

## I. Dataset location & Content

For our attack propagation analysis [1], the dataset can be found at [2]. It contains a readme, which summarise the most important points of executing the analysis and what the expected results are. Additional information and the current source code can be found at our Github repositories: Metamodel[1], Analysis[2], and the Eclipse Product[3].

## II. Executing the Product

We provide a VM image with an Eclipse Product, which can be used to start our analysis and view the models. It is configured to open a workspace automatically with the necessary projects. The necessary steps after downloading the dataset and unzipping it are:

- After extracting the VM image is in *binary/vm*. We tested the image with VirtualBox 6.1.
- In the VM the product is in the home directory under *AttackerPropagation*. The credentials for the VM are:
  - User: icsa
  - Password: icsa
  - Root-Password: icsa
- The product can be executed by using the *PalladioBench* binary (not the eclipse binary!)
- After the load screen, there are are 3 projects in the Modelviewer on the left side. These contain the tests for the evaluation and the used models.
- The test project contains also automatic test cases for the accuracy evaluation goal. The test can be executed by opening the context menu (right click usually) and "Run as" Junit-Plugin-Test. It is important to execute the tests as Plugin Tests since otherwise the dependencies cannot be solved

There are also binaries available for usage without the VM and the source code of the analysis is available. The usage for these is described in the readme of the dataset [2].

### A. Result Interpretation

The expected results can be found in the *evaluationmodel* folder. The folder contains all the necessary input and the expected output models for each investigated case study. The description of the case studies can be found in [1] and the readme. The ids of the non pcm elements (*ServiceRestrictions* and *CompromisedData*) might change for every analysis run since they are dynamically calculated. However, the other properties of these elements are stable and can be used for comparison. For documentation regarding the modelling of the software architecture, please look at the Palladio book [3]. It describes where the architectural elements are modelled.

## Acknowledgement

This work was supported by the German Research Foundation (DFG) under project number 432576552, HE8596/1-1 (FluidTrust), as well as by funding from the topic Engineering Secure Systems (46.23.03) of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

## References

[1] M. Walter, R. Heinrich, and R. Reussner, "Architectural attack propagation analysis for identifying confidentiality issues," in *ICSA'22*.

[2] ——, "Dataset - architectural attack propagation analysis for identifying confidentiality issues," [Online]. Available: https://doi.org/10.5445/IR/1000141655.

[3] R. Reussner, S. Becker, J. Happe, *et al.*, *Modeling and Simulating Software Architectures – The Palladio Approach*. Cambridge, MA: MIT Press, Oct. 2016, 408 pp.

[1] https://github.com/FluidTrust/Palladio-Addons-ContextConfidentiality-Metamodel

[2] https://github.com/FluidTrust/Palladio-Addons-ContextConfidentiality-Analysis

[3] https://github.com/FluidTrust/Palladio-Bench-Product-AttackerPropagation