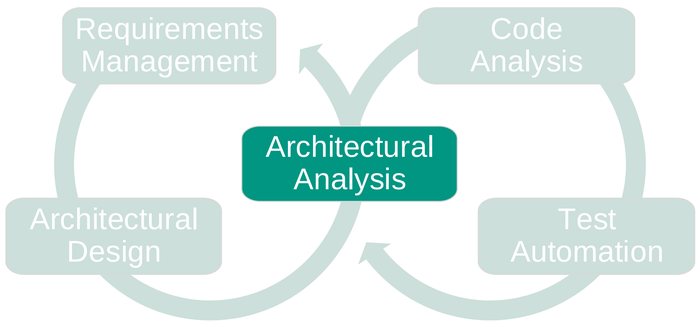
Karlsruhe Institute of Technology

HELMHOLTZ

Towards Architectural Pen Test Case Generation and Attack Surface Analysis to Support Secure Design



RG and Labs: Mobility Lab

Contributors: Mahdi Jafari Sarvejahani (Dependability), Dr. Christopher Gerking (Dependability), Prof. Dr. Ralf Reussner (Dependability).

Motivation and Research Questions

The lack of assessment on the design decisions made by software architects leads to critical vulnerabilities in the architecture, ultimately resulting in insecure software. This absence motivates us to contribute through three main RQs:

- **RQ1.** How can **architectural penetration test cases** be generated based on architectural models during the design phase?
- **RQ2.** How can the generated test cases be prioritized to facilitate penetration testing efforts?
- **RQ3.** How can generated test cases be used to **identify security risks and rate architectural models** based on their security levels?

Impact

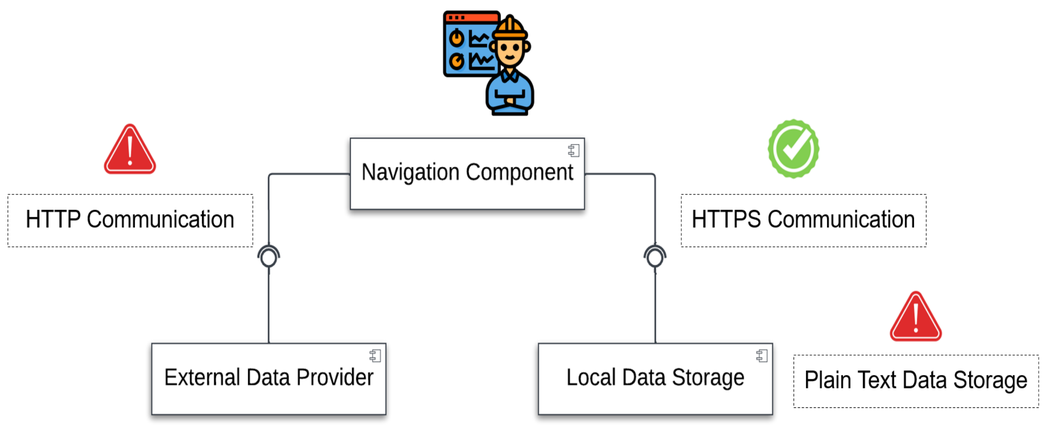
For Architects: Early security feedback to avoid insecure design choices.

For Pen Testers: Pre-generated penetration test cases reduce manual effort.

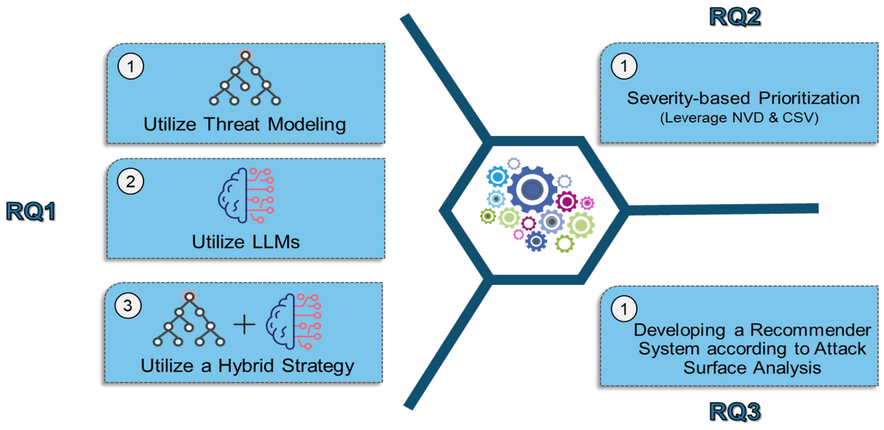
For Industry: Cost savings via "security by design" adoption + Resulting in more secure vehicles.

Research Activities and Results

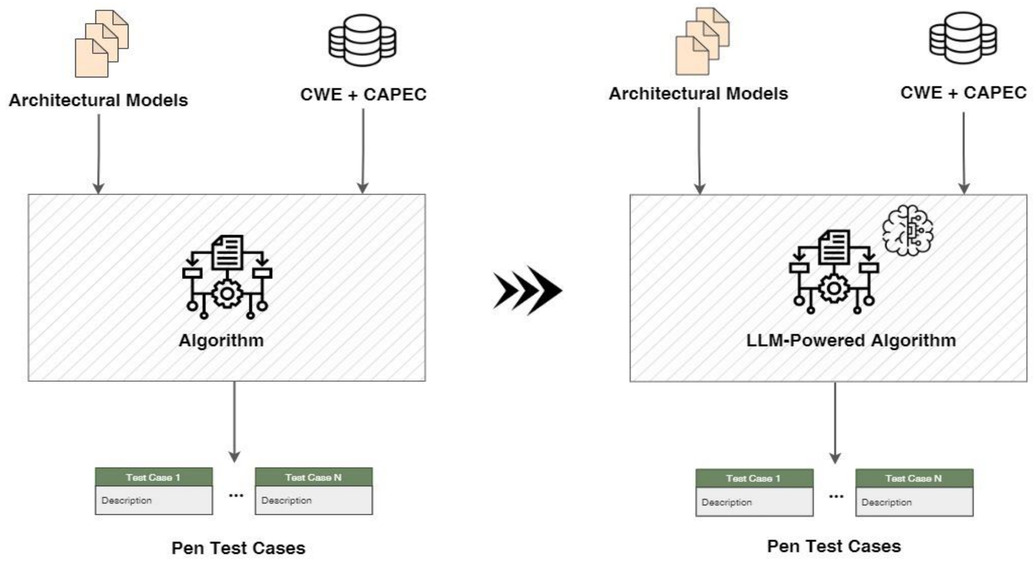
Early design decisions and security: What is the correlation?



Preliminary Strategies



Pen Test Case Generation by Utilizing LLMs



Next Steps

- Identify different type of Attackers, their motivation, behavior, and capabilities.
- Gain a deeper understanding of the Pen Test Case Generation process used by penetration testers.
- Better understand design decision-making process.

Publications

- [1] M. Jafari Sarvejahani, “Towards architectural pen test case generation and attack surface analysis to support secure design,” 22nd IEEE International Conference on Software Architecture (ICSA 2025), Odense, Denmark, 2025.

links to: Engineering Security for Mobility Systems; Methods for Design & Development

KASTEL