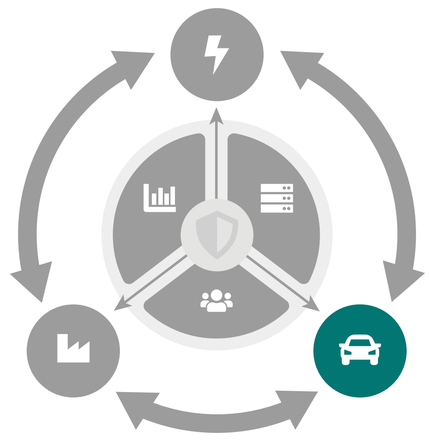
Karlsruhe Institute of Technology

P1T3

Vulnerability Discovery for Highly-Configurable Software Systems



T. Bächle, E. Hofmayer, C. König, T. Pett, I. Schaefer
(Mobility Systems Security, Software Engineering)

Motivation and Research Questions

- **Vulnerabilities** are difficult to identify and can have drastic consequences
- **Query-Based Static Application Security Testing (Q-SAST) tools** promise great benefits for vulnerability discovery
- **Highly-Configurable Software Systems**, i.e., Software Product Lines (SPLs), are becoming **common** in many domains (e.g., mobility)
- **Q-SAST tools cannot be applied to SPLs without further adjustments**

➡ How can the benefits of Q-SAST be leveraged for the scalable analysis of real-world SPLs for the presence of common vulnerability patterns?

Impact

- **Resource demand** of analysis feasible for practical use
- **Dangerous** code **patterns can be identified early**
- **Consequences of exploitation can be averted**

Real World Example

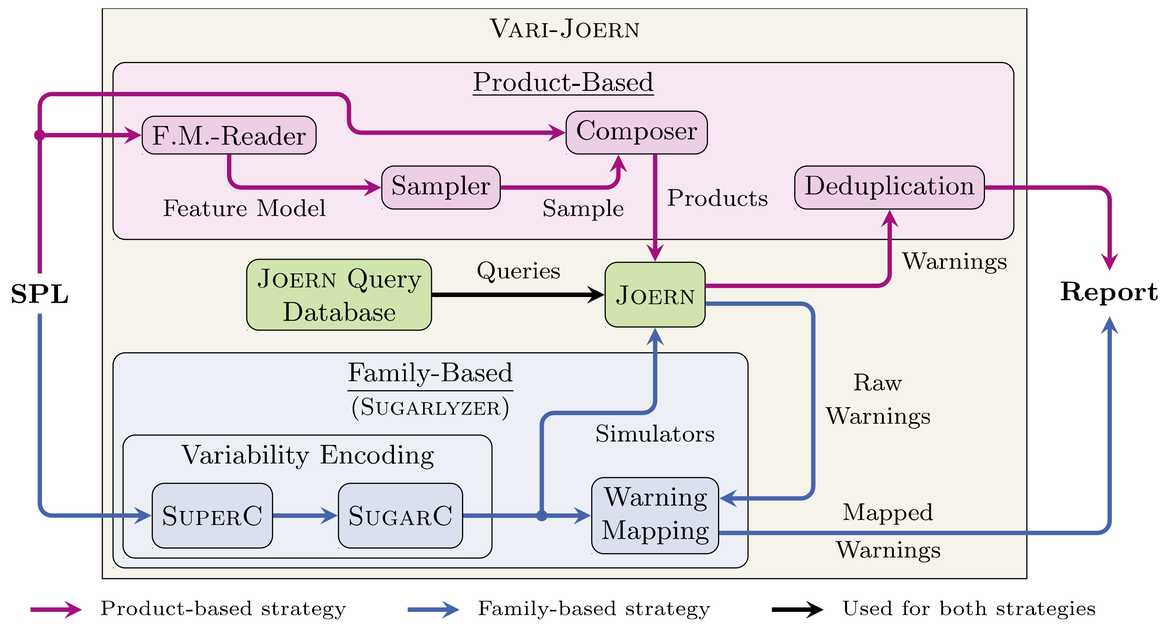
```
#ifndef OPENSSL_NO_HEARTBEATS
  // [...]
  n2s(p, payload);
  // [...]
  if (hbtype == TLS1_HB_REQUEST){
    unsigned char *buffer, *bp;
    // [...]
    buffer = OPENSSL_malloc(1 + 2 +
      payload + padding);
    bp = buffer;
    // [...]
    memcpy(bp, pl, payload);
    // [...]
  }
  // [...]
#endif
```

Heartbleed Vulnerability

Research Activities and Results

An analysis platform using the powerful Q-SAST tool Joern for vulnerability discovery in SPLs

- **Product-Based Analysis:** Sample a set of representative software products from the SPL
- **Family-Based Analysis**: Transform (variability encode) the variable SPL source code into plain source code



Results:

- **Analyzed** multiple **real-world SPLs** for vulnerabilities
- **Identified potentially dangerous** code **patterns**

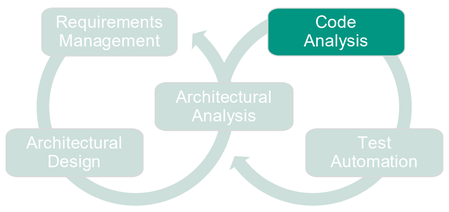
Roadmap:

- Support for **additional subject systems** in Vari-Joern
- **Address limitations** of solutions reused in Vari-Joern
- Enable Joern to **analyze SPLs** for vulnerabilities **directly**

Publications

- Family-based Vulnerability Discovery for Software Product Lines. Master's thesis 2024.
- Sampling-Based Vulnerability Analysis using Joern. In: Bachelor's thesis 2025.
- Investigating the Effects of T-Wise Interaction Sampling for Vulnerability Discovery in Highly-Configurable Software Systems. In: SPLC 2025 (under review).

links to:



KASTEL