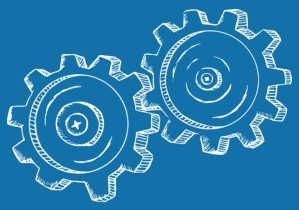

Bug Discovery in System-Level Software

Advisor: **Lorenz Schumm**

Motivation

Modern software systems are becoming more and more complex, with the Linux Kernel reaching 40 million lines of code in 2025. With the increasing complexity comes an increase in the amount of security bugs. Finding these bugs manually is impractical at this scale.

This project focuses on analyzing modern system-level software and creating tools to aid developers in finding and fixing security bugs. The tools developed could help identify memory corruption issues, privilege escalation vulnerabilities, or race conditions in system-level components. Such tools have real-world impact, potentially securing software running on billions of devices.

The project scope is fairly open and will be discussed based on experience and interest. Whether focusing on Android's native components, kernel drivers, or specific vulnerability classes, we will find something that fits you. You'll learn about cutting-edge static program analysis techniques.

Goals and Tasks

- Review prior work on advanced static analysis methods.
- Explore new methods of finding and analysing bugs in complex, system-level software.
- Implement new analysis tools,
- Or extend existing ones with new mechanisms, such as LLM support.

Literature

- X. Wang et al.
  {ZIPPER}: Static Taint Analysis for {PHP} Applications with Precision and Efficiency
  USENIX Security
- R. A. Popa and F. Flynn
  Introducing CodeMender
  https://deepmind.google/discover/blog/introducing-codemender-an-ai-agent-for-code-security/

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Basic operating system knowledge
- (C/C++, Python) experience
- Information Security course
- Interest in system security

Advisor Contact

lorenz.schumm@tugraz.at