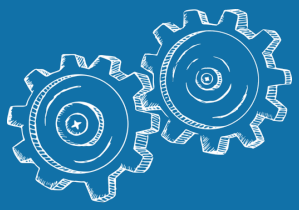

Fuzzing System-Level Software

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. Traditional testing approaches cannot cover the vast input and execution spaces of such systems.

This project focuses on developing advanced fuzzing techniques for modern system-level software. The research will involve creating intelligent fuzzers that can navigate complex system interfaces, generate meaningful inputs for kernel subsystems or Android components, and efficiently explore deep execution paths. These techniques are essential for discovering critical vulnerabilities like memory corruption, use-after-free, or concurrency bugs before they can be exploited.

The project scope is flexible and will be tailored based on interests and prior experience. Potential directions include state-guided fuzzing of kernel drivers, feedback-driven fuzzing of Android native services, or hybrid approaches combining LLMs with fuzzing.

Goals and Tasks

- Review prior work on fuzzing for specific targets.
- Explore new methods of automatically testing a specific target.
- Explore ways of enhancing existing methods using modern tools such as LLMs.
- Extend existing fuzzing frameworks to identify and analyse previously unknown security issues.

Literature

- P. Mao, M. Busch, and M. Payer
  {NASS}: Fuzzing All Native Android System Services with Interface Awareness and Coverage
  USENIX Security
- Y. Yang et al.
  Hybrid Language Processor Fuzzing via {LLM-Based} Constraint Solving
  USENIX Security

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
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