



Kernel Taint Tracking

Advisor: **Lukas Maar**

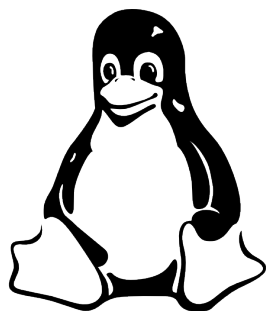
Motivation

Taint tracking in the Linux kernel is a mechanism that can be used to track the flow of untrusted or potentially harmful user data. It serves a dual purpose in cybersecurity: defense and offense. Defensively [2], it carefully monitors user data flow to protect the kernel from threats. On the other hand, attackers [1] find it valuable as it reveals potential objects that can be used for kernel exploitation. This makes taint tracking a key factor in modern kernel security.

This project will further investigate the possibility of using a static analyzer for taint tracking within the Linux kernel. Recognizing the capability of the LLVM compiler as a framework for such analysis, we intend to develop a proof-of-concept. This LLVM-based approach aims to automatically analyze the kernel, unveiling the flow of untrusted or potentially harmful user data.

Goals and Tasks

- 📖 Get familiar with the Linux kernel's and LLVM compiler's infrastructure
- ✂️ Develop a compiler pass that performs taint tracking in the Linux kernel
- 💡 Demonstrate and evaluate the implementation



Literature

- > [Z. Lin et al.](#)
GREBE: Unveiling Exploitation Potential for Linux Kernel Bugs
[S&P](#)
- > [R. Wang et al.](#)
AlphaEXP: An Expert System for Identifying Security-Sensitive Kernel Objects
[USENIX 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

- > Programming: C/C++
- > Interest in the Linux kernel
- > Interest in compiler technology and system security

Advisor Contact

lukas.maar@iaik.tugraz.at