Gilbert Hoermann

www.seal9055.com | seal9055@gmail.com | https://github.com/seal9055 | linkedin.com/in/gilberthoerm

Objective

Experienced in systems-security, compilers, computer architecture, operating systems and automated program analysis for benchmarking and bug-hunting. Looking to use these skills to break into the HFT industry.

Experience

Trail of Bits Vulnerability Research Internship 01/2023 - 02/2023

- Designed and implemented an efficient coverage guided graybox snapshot fuzzer on top of Qemu
- The fuzzer scaled linearly while communicating various forms of data across hundreds of cores

UMass Computer Science Lecturer - *https://umasscybersec.org/cs390r.html* 01/2022 - 05/2023

- Teaching a course on reverse engineering and advanced vulnerability analysis to a class of 55 students
- Topics include re/code auditing, fuzzing, stack/heap exploitation, kernel-mode security, and automated dynamic/static software analysis w/ llvm, decompiler scripting, taint analysis, pin, and time-travel dbg

Projects

Fuzzing Research using Emulation/JIT - *https://github.com/seal9055/sfuzz* 09/2021 - 07/2022

- Wrote an emulation-based greybox fuzzer focused on performance, code coverage and scaling
- The emulator + custom JIT enable high levels of target introspection without requiring source code
- The fuzzer includes coverage guided seed selection, byte level permission checks, snapshot fuzzing, custom high performance memory allocation routines, and scales linearly across cores

C++ Backtesting Framework 07/2023 - Current

- Wrote a small C++ backtesting framework and used it to implement some simple low indicator strategies based on historic tick and candle data.
- Evaluated model based on indicator entropy, beta convergences and overall results and attempted some non-linear strategies

Low Latency Benchmarking OS-Development 08/2022 - 12/2022

- Worked on a custom OS focused on producing deterministic/no-jitter benchmarking results
- Implemented Numa-aware memory distribution between cores with a no-shared-memory model, allowing the cores to perform lock-free concurrent work while communicating through message pipes

Skills

- Benchmarking (Custom profiling OS and standard solutions such as Intel VTune/Google Benchmark)
- Cpp optimization (move semantics, comp-time dispatch, cache locality, concurrency)
- Numa-locality aware OS development for memory profiling and benchmarking
- Computer Architecture Concepts such as caches, pipelining, simd, and hyper-threading
- Compiler Optimizations from writing llvm passes and developing custom JIT compiler architectures
- Reading, Writing and manually optimizing Assembly (x86, arm, mips & riscv)
- Reverse engineering, static program analysis (llvm), and dynamic analysis (pin, gdb, triton, unicorn)

Education

University of Massachusetts Amherst 08/2020 - 05/2023

- Graduated with BS in computer science with a focus on systems and security - GPA 3.8

Certifications & Achievements

OSCP - January 2021 **Sans Foundations** - June 2021

Ret2 Systems Binary Exploitation Course - *wargames.ret2.systems/course* 03/2021

Hypervisor Development for Security Researchers Course - *https://tandasat.github.io/* 08/2022