

Gilbert Hoermann

www.seal9055.com | seal9055@gmail.com | <https://github.com/seal9055> | [linkedin.com/in/gilberthoerm](https://www.linkedin.com/in/gilberthoerm)

Education

University of Massachusetts Amherst - Expected Graduation: May 2023

- 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

CtfTime Top 7 US - Binary exploitation player for k3rn3l4rmy

Experience

Trail of Bits Vulnerability Research Internship

01/2023 - Current

- Working on a project to integrate sfuzz into the unicorn emulation engine to perform differential fuzzing across multiple targets using dirty-bit based snapshot-fuzzing for high performance

UMass Cybersecurity Lecturer - <https://umasscybersec.org/cs390r.html>

01/2022 - Current

- 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

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, memory allocation hooks and linear scaling across cores without a source requirement

Technical Director at UMass Cybersecurity Club

11/2021 - Current

- Hosting workshops focused on low level security topics such as binary exploitation and fuzzing
- Created virtualized enterprise network as training grounds for CPTC pentesting competition

Projects

Wyze Camera - CVE-2021-43726 & CVE-2021-43727

- Reverse engineered and emulated (using qemu) device's firmware to find and exploit 2 critical bugs
- Rce via format string bug and remote image/video download by attackers via path traversal

Website to Publish Ctf Writeups and Blog Posts - seal9055.com/

- Writeups cover stack/heap/kernel/browser exploitation, reverse engineering, and fuzzing
- Blog-series on Chrome exploitation covering relevant V8 internals and exploitation techniques
- The blog is used document my studies and provide educational material for readers

Officejet Pro 6835 - https://github.com/seal9055/officejet_pro_6835

(In progress)

- Project to find rce in popular printer. Currently extracting firmware through multiple layers of non-standard compression/encryptions that binwalk could not handle

Skills

- Reverse engineering, static analysis (binary ninja, llvm), and dynamic analysis (pin, gdb, triton, unicorn)
- Exploit dev, writing n-day (and ctf) exploits for userland, kernel (Linux), and browser (Chrome) bugs
- Bug discovery techniques, fuzzer harnessing, dataflow-analysis, patch diffing and variant analysis
- Understanding of modern exploit mitigations (ASLR, SMAP, HVCI, Sandboxing, ...) and bypass strategies
- Systems programming in the context of writing high-perf emulators, kernels, compilers and hypervisors
- Embedded VR, extracting firmware from flash, reversing decompression, emulation/fuzzing setup
- Ability to quickly tackle and get familiar with unfamiliar large codebases and binaries