# Gilbert Hoermann

www.seal9055.com | seal9055@gmail.com | https://github.com/seal9055 | 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 3.7

## Certifications & Achievements

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

**Ctftime Top 7 US** - Binary exploitation player for k3rn3l4rmy

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

**Hypervisor Development for Security Researchers Course** - Satoshi Tanda 08/2022

## Experience

**Trail Of Bits Winternship** 01/2023 - 02/2023

- Working on a project focused on browser security and the efficacy of different fuzzers (nyx, wtf, libafl)

**UMass Cybersecurity Lecturer -** *https://umasscybersec.org/cs390r.html* 01/2022 - 05/2022

- Teaching a course on reverse engineering and advanced vulnerability analysis to a class of 50 students
- Topics include re/code auditing, fuzzing, heap based exploitation, kernel-mode security, and automated dynamic/static software analysis using llvm passes, taint analysis, pin, and time travel debuggers

**Ret2 Systems independent security contractor** 10/2021 - 01/2022

- Tasked with creating low level security challenges to be used as educative material
- The challenges covered reverse engineering, binary exploitation and cryptography

**Fuzzing Research focused on Emulation -** *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
- Creating 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 poc 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

- Vulnerability research using static analysis (llvm, (win)gdb, ida), and dynamic analysis (fuzzers, pin, z3)
- Exploit dev, patch diffing and variant analysis for windows/linux kernel & userland and browsers
- Understanding of modern exploit mitigations (ASLR, SMAP, HVCI, ...) and bypass strategies
- Systems programming in the context of writing emulators, osdev, compilers and hypervisors
- Reverse engineering and VR on embedded devices to extract firmware and setup fuzzing environments