

Aaron Lichtman

SOFTWARE ENGINEERING · CYBERSECURITY

✉ aaronlichtman@gmail.com | 🏠 alichtman.com | 📧 alichtman | 🌐 aaron-lichtman

Experience

Security Engineer

Seattle, WA

PRODUCT SECURITY (NATIVE ASSURANCE) — META

June 2022 - Present

- Created threat models and documented attack surfaces in order to effectively prioritize security review efforts.
- Conducted security reviews of high-risk surfaces. Implemented mitigations that eliminated vulnerabilities.
- Triageed whitehat reports, awarded bug bounty payouts, and created proof of concept exploits.
- Built systems to detect and prevent security issues before they are deployed.

Rotational Security Engineer

Remote

RED TEAM X, INCIDENT DETECTION & RESPONSE (IDR), PRODUCT SECURITY — META

April 2022 - June 2022

- Expanded EDR capabilities, improved case investigation tooling, and triaged the incident queue.
- Expanded coverage of automated vuln detection tools.
- Coordinated incident response at company-wide scale (including **log4j**).
- Created signatures to identify and block malware.

Software Engineer

Remote

PORTAL KERNEL SECURITY — FACEBOOK

Sept 2020 - April 2022

- Led hardening efforts for **PortalOS** by using sanitizers, fuzzers, and modern security mitigations.
- Built fuzzing harnesses using **AFL**. Used **UBSAN** / **ASAN** / **MSAN** / **TSAN** to find hundreds of bugs, including a set of memory corruption vulnerabilities in **PJSIP**: **CVE-2022-39244** (9.8 CVSS).
- Added Portal support to manufacturing platform. Built HSM integration, logging for security auditing, auto-escalation policies.
- Created factory resource monitoring systems to eliminate resource-related manufacturing issues, saving millions of dollars.

Software Engineering Intern

Menlo Park, CA

AUTHENTICATION E2E TEAM — FACEBOOK

Summer 2019

- Worked on a team securing authentication across the entire Facebook universe of apps, including Whatsapp and Instagram.
- Designed, implemented and deployed a solution to prevent internal attackers from obtaining access to user accounts and data.
- Improved monitoring and auditing capabilities in C++ for more than 1 billion daily authentication attempts.

Open Source Software

Malware Techniques

2019

A COLLECTION OF TECHNIQUES USED IN LINUX AND MACOS MALWARE

- Researched Linux and macOS malware, and implemented anti-VM, anti-debugging, anti-analysis and persistence measures.
- Designed a **Linux LKM (4.6 - 4.18)** rootkit that hooks syscalls and is undetected by standard rootkit checkers.
- Developed educational malware in a variety of languages, including: C, x86, Bash, Python, and Objective-C.

Deadbolt

2019

DEAD SIMPLE FILE ENCRYPTION

- Built a cross-platform desktop Electron app with a sleek UI to simplify encryption and decryption of files.
- Designed an intuitive user experience for secure encryption with **AES-256**, easily accessible to non-technical users.

Stronghold

2018

MACOS HARDENING TOOL

- Developed software that guides users through step-by-step secure configuration for macOS.
- Secured more than **70k** macOS workstations, earned over **1k** stars on GitHub.

Education

University of Illinois at Urbana-Champaign

Champaign, IL

B.S. IN COMPUTER SCIENCE AND LINGUISTICS

May 2020

- **GPA:** 3.54/4.00; **Dean's List:** 2017, 2018, 2019, 2020
- Discrete/Data Structures, Algorithms, Computer Architecture, Systems Programming, Computer Security, Digital Forensics

Skills

Certs

OSCP

Languages

Python, C, C++, Swift, x86, Node.js, bash / zsh, AppleScript

Tools

macOS, Linux, Ghidra, Wireshark, VMware / VirtualBox, Volatility, Git