Aaron **Lichtman**

Security and Software Engineer

aaronlichtman@gmail.com | alichtman.com | alichtman | aaron-lichtman

Experience

Software Engineer — *Seattle, WA*
VS Code Team — Meta — *August 2023 - Present*

- Core maintainer of the primary IDE used by Meta engineers, improving developer productivity across the company.
- Contributed open source fixes upstream to the VS Code project and its dependencies.

Security Engineer — *Seattle, WA*
Product Security (Native Assurance) — Meta — *June 2022 - August 2023*

- 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.
- Triaged whitehat reports for the bug bounty program, established payout guidelines, and created proof of concept exploits.
- Built systems to detect and prevent security issues before they reach production.

Security Engineer — *Remote*
Red Team / Incident Detection & Response (IDR) — Meta — *April 2022 - June 2022*

- Expanded EDR capabilities, improved case investigation tooling, and triaged the incident queue.
- Worked the incident response oncall, and coordinated response at company-wide scale.
  - Including patching `log4j` on day 0 for critical services.
- Reverse engineered malware, and created signatures to automatically identify and prevent it from running.

Software Engineer — *Remote*
Kernel Security for Facebook Portal (Android-based Video Conferencing Device) — Meta — *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 PJSIP memory corruption vulnerabilities: `CVE-2022-39244 (9.8 CVSS)`.
- 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.

iOS Software Engineering Intern — *Boston, MA*
iOS Core Team — Wayfair — *Summer 2018*

- Developed a furniture sharing iMessage extension in Swift for the Wayfair iOS app.
- Addressed challenging iOS security issues, balancing customer experience and data security.

CS125 Course Developer — Plagiarism Detection Software — *Champaign, IL*
University of Illinois CS Department (working with Asst. Prof. Geoff Challen) — *2018*

- Designed plagiarism detection software that applies machine learning to code metrics and behavioral indicators.
- Analyzed natural language and performed static analysis using NLTK and ANTLR.

CS125 Course Assistant — Java Programming Fundamentals — *Champaign, IL*
University of Illinois CS Department (working with Asst. Prof. Geoff Challen) — *2017*

- Taught fundamentals of Java programming, algorithm design, and data structures in weekly two-hour lab sections.
- Worked one-on-one with students in office hours to help them develop a deeper understanding of computer science.

Open Source Software

Malware Techniques — *2019*
A library of Linux and macOS malware techniques

- Researched Linux and macOS malware, and implemented anti-VM, anti-debugging, anti-analysis and persistence measures.
- Designed a Linux kernel (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.

Stronghold — *2018*
macOS Hardening Tool

- Developed software that guides users through step-by-step secure configuration for macOS.
- Secured `56k+` macOS workstations; earned over `1k` stars on GitHub.

shallow-backup
Open Source Software — *2018*

- Developed a tool for developers to easily create backups of installed packages and dotfiles, and automatically push them to a remote Git repo.
- Used by `70k+` developers to minimize system backup size; earned over `1k` stars on GitHub.

Education

University of Illinois at Urbana-Champaign *Champaign, IL*

B.S. in Computer Science and Linguistics *May 2020*

- Graduated with honors. Included on the Dean's List: 2017, 2018, 2019, 2020
- **Courses**: Discrete/Data Structures, Algorithms, Computer Architecture, Systems Programming, Computer Security, Digital Forensics

Skills

Certs OSCP

Languages Python, C / C++, Node.js, bash / zsh

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