

Richard Liu

rjliu@protonmail.com | +1 (408) 386-2085
Champaign, IL (open to relocation) | github.com/richyliu
rliu.dev | linkedin.com/in/richard-liu-4775571a7

Publications

BAR Workshop (NDSS '26) – RT-Fuzzer: Task Driven Fuzzing of Real Time Operating System Firmware Feb 2026

- Contributed setup, debugging, and evaluation of RT-Fuzzer on Apache NuttX.
- Discovered multiple critical vulnerabilities (CVE-2025-48768, CVE-2025-48769) in filesystem and FTP components, enabling denial-of-service and potential remote code execution.

IEEE INNOVARail 2026 – SAFE-T: Secure Authentication Framework for End-of-Train Communications Jan 2026

- Identified and demonstrated a critical cybersecurity vulnerability in the radio communication protocol used by freight train End-of-Train Devices (EOTDs).
- Showed that an brake commands could be transmitted by anyone with a low-cost software-defined radio.

Experiences

Trail of Bits – Software Engineer Intern

Oct 2025 - Dec 2025

New York, NY (remote)

- Audited and instrumented Google's V8 runtime to uncover potential memory-safety and sandbox-escape vulnerabilities in WebAssembly stack switching and JS builtins
- Reverse-engineered engine internals and developed proof-of-concept exploit paths (stack metadata corruption, builtin misdispatch), producing detailed security findings and recommendations

Trail of Bits – Software Engineer Intern

Dec 2024 - Jan 2025

New York, NY (remote)

- Profiled and optimized pwndbg, a popular Python GDB plugin, reducing startup time by 15% and cutting load time for core functionality by 85% for thousands of users worldwide.

Battelle Memorial Institute – Cyber Security Intern

May 2024 - Aug 2024

Columbus, OH

- Designed and implemented a distributed over-the-air fuzzing system, scaling fuzz testing across multiple devices and leading to 10x increase in fuzzing throughput.
- Developed Python-based fuzzing tools targeting embedded wireless stacks; reverse-engineered Bluetooth chipsets to expose internal commands for better fuzz testing integration and testing.

Sandia National Labs – R&D Software Intern

May 2023 - Dec 2023

Albuquerque, NM

- Reverse-engineered embedded firmware with Ghidra to discover security vulnerabilities in binaries.

Education

University of Illinois Urbana-Champaign – M.S. in Computer Science

Aug 2024 - May 2026 (anticipated) | GPA: 3.9/4.0

Champaign, IL

- Research topics: Embedded firmware, fuzz testing, cyberphysical/OT security
- Projects include a libfuzzer + QEMU integration written in C for binary-only firmware fuzzing, a ZeroMQ device model for QEMU to enable generic peripheral interactions, and a firmware-in-the-loop integration between Halucinator and OT-Sim written in Python and C.

University of Illinois Urbana-Champaign – B.S. in Mathematics & Computer Science

Aug 2021 - May 2024 | GPA: 3.9/4.0

Champaign, IL

Technical Skills

- **Expert:** Python, C, fuzz testing, OOP, JavaScript, data processing, Assembly (x86, ARM, MIPS, RISC-V), Git
- **Proficient:** Docker, IoT, TCP/IP, Kubernetes, Cloud infrastructure, PostgreSQL