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.
- Designed and proposed a backward-compatible, authenticated extension to the existing EOTD communication protocol, effectively mitigating the vulnerability while remaining compatible with current-generation hardware through minor software modifications.

Experiences

Trail of Bits – *Software Engineer Intern*
Oct 2025 - Dec 2025 New York, NY (remote)

- Conducted a security audit of Google V8 JavaScript/WebAssembly engine, analyzing JS/Wasm interop, stack switching (JSPI), and runtime invariants to identify potential memory corruption and sandbox escape vulnerabilities
- Reverse engineered and instrumented V8 internals (TurboFan/TurboShaft, builtins, isolate stack management) with custom runtime tracing to validate control-flow, stack state, and exception-unwinding behavior
- Developed and tested exploit hypotheses (stack metadata corruption, TOCTOU on callables, builtin confusion), demonstrating cross-builtin control-flow redirection and mapping high-risk trust boundaries

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.
- Applied Python profiling tools (cProfile, line_profiler) to diagnose bottlenecks in large codebases.

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.
- Built a remote firmware debugger with Python and instruction patching, requiring a deep knowledge of the underlying firmware binary.
- Enabled colleagues to diagnose firmware more effectively, improving the lab’s embedded analysis capability and decreased overall debugging time by 30%.

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.

Relevant coursework: Machine Learning for Signals Processing, Data Structures & Algorithms

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

Aug 2021 - May 2024 | GPA: 3.9/4.0 Champaign, IL

Relevant coursework: Cryptography, Computer Systems Engineering

Competitions

MITRE eCTF – *2nd place*

2022-2024

- Top embedded cyber competition hosted by MITRE. Earned 2nd place nationwide (out of 30+) in 2023.
- Led 20 students across 3 subteams to design a secure car key fob system; implemented encryption/authentication schemes and mitigated replay attacks.
- Developed project management and leadership skills, coordinating efforts across subteams.
- Personally discovered and exploited an ARM buffer overflow.

CSAW CTF – *3rd place*

2022-2024

- Annual top-tier national cyber competition hosted by NYU Tandon
- 2022: 5th place nationwide.
- 2023: 3rd place nationwide.

Projects

UIUCTF 2024 Infrastructure

- Use Docker and Kubernetes to deploy a scalable infrastructure for the UIUCTF 2024 competition, supporting over 4000 participants.
- Gained valuable experience with GCP cloud infrastructure tools and Terraform.

ZeroMQ/QEMU Integration

Research Project

- Implemented a C-based pubsub ZeroMQ device model for QEMU, enabling generic peripheral interactions.
- Improved peripheral simulation throughput by 2–10x compared to Python-GDB approaches.

OT-Sim/Halucinator Integration

Research Project

- Bridged firmware rehosting (Halucinator) with physical system simulation (OT-Sim), solving synchronization and message translation challenges.
- Delivered a firmware-in-the-loop PoC for a PLC motor controller integrated into a wind turbine simulator.
- Used Python, C, and Docker to create a seamless interface between rehosted firmware and simulated physics environment.

QEMU Snapshot Fuzzer

Summer Project

- Developed a QEMU + libFuzzer integration for binary-only firmware fuzzing with coverage feedback.
- Enabled fuzz testing of proprietary firmware blobs in critical sectors (industrial, aerospace).

PreHeat

Group Term Paper

- Built an optimizer to explore design parameters for Fully Homomorphic Encryption (FHE) accelerators.
- Integrated cycle, power, and area simulations to identify optimal configurations, improving scalability of accelerator designs.

UIUC Apartments

Group Project

- Built a web platform with cloud infrastructure backend aggregating local housing data via custom Python scrapers, PostgreSQL backend, and GCP Cloud Functions.

- Adopted by hundreds of UIUC students to find apartments.

Misc

No work authorization needed in the U.S. Able to obtain a U.S. security clearance.

Last updated: March 2026

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