

Richard Liu

Email: rjliu3@illinois.edu

Location: Cupertino, CA (open to relocation)

Github: github.com/richyliu

Phone: (408) 386-2085

Linkedin: [linkedin.com/in/richard-liu-4775571a7](https://www.linkedin.com/in/richard-liu-4775571a7)

Personal website: rliu.dev

EDUCATION **University of Illinois at Urbana-Champaign** August 2021 - May 2025 (anticipated)
B.S. in Mathematics & Computer Science 4.0/4.0 GPA

EXPERIENCE **TITANS CCD Intern** — *Sandia National Labs* May 2023 - Present

- Reverse engineered embedded systems using Ghidra
 - Performed dynamic analysis through creative use of diagnostic memory primitives and crash vectors
 - Low level binary exploitation
 - Red team attacks on power systems
- Created automated pentesting suite for 5G networks
 - Tested various parts of 5G network stack

Embedded Systems Research — *SPRAI* April 2022 - June 2022

- Used QEMU snapshot fuzzer from GSoC to fuzz test PLCs
- Wrote a paper on feasibility of snapshot fuzzing in QEMU

QEMU — *Google Summer of Code* June 2022 - September 2022

- Developed a snapshot/restore fuzzer for QEMU as part of my Google Summer of Code project
- Integrated Libfuzzer test harness and coverage information from within QEMU

SIGPwny club admin — *UIUC* Fall 2022 - Present

- Organized our club's participation in eCTF, MITRE's annual embedded security competition, in which we placed third overall

AWARDS **CSAW** — *New York City, New York* November 2022
NYUSEC

- Competed on a team of 4 in a cybersecurity competition (CTF)
- Placed second place nationwide in the undergraduate division

SKILLS **Reverse engineering/binary exploitation** (Ghidra, pwntools, GDB)
Linux & Systems Programming (Rust, Bash, C, C++)

PORTFOLIO **UIUC Apartments:** Apartment hunting website for my local area. Scraped data with Python and used PostgreSQL + GCP Cloud Functions for the backend.
QEMU Snapshot Fuzzer: QEMU fork with snapshot/restore features and libfuzzer integration