Zheng Yu

zheng.yu@northwestern.edu | github.com

Education

Northwestern University
Ph.D. Student in Computer Science — *Sept. 2022 - Present*

Shanghai Jiao Tong University
Bachelor of Computer Science in Computer Science, member of ACM Class — *Sept. 2018 - June. 2022*

Research Experience

Research Intern — Feb. 2022 – July. 2022
Northwestern University, USA — *Mentors: Xinyu Xing*

- As a research intern in Northwestern University advised Prof Xinyu Xing.
- Focused on designing next-generation memory corruption protection mechanism.
- Also worked on static analysis of kernel source code.

Student Intern — June. 2021 – Jan. 2022
JD.com, Inc. — *JS Security*

- As a student intern at the Qiling team on JD.com.
- Focused on microcontroller (MCU) firmware emulation.
- As a core developer of Qiling binary analysis framework.

Research Intern — Feb. 2021 – April. 2021
Southern University of Science and Technology — *Mentors: Yinqian Zhang*

- As a research intern in SUSTech advised by Prof Yinqian Zhang.
- Focused on the design of remote attestation protocol on distributed TEE systems.
- Develop and improve RISC-V trusted computing platform Keystone-Enclave.

Undergraduate Research Assistant — July 2020 – 2022
Sustainable Architectures and Infrastructure Laboratory (SAIL) — *Mentors: Chao Li*

- As an undergraduate research assistant in the SAIL lab advisied by Prof Chao Li.
- Focused on data center systems and architectures design and cloud computing power management.
- Prof Chao Li's evaluation of me is "He has the potential to become an outstanding graduate student"

Talks

- **Zheng Yu**, KAI JERN LAU, MuChen Su, Anh Quynh NGUYEN.
  Reversing MCU with Firmware Emulation, BlackHat Europe 22.

Teaching Experience

Student Mentor — Apr. 2022 – Oct. 2022
Google Summer of Code 2022

- As the student mentor of Qiling Improvements projects in GSOC 2022.
- Focused on bridging qiling with other reverse engineering tools (e.g. r2, ghidra).
- Discuss and provide guidance to developers involved in the project.

Teaching Assistant — June. 2019 – Sept. 2019
Shanghai Jiao Tong University

- As teaching assistant in Programming Design Course (CS151) in SJTU
- Design programming assignments and course projects for students
- Students think I am a helpful and responsible teaching assistant

Honors & Awards

7th at Defcon 22 CTF Finals DEFCON
StrawHat Team *2022*

Outstanding graduates SJTU
Outstanding Graduate of Shanghai Jiaotong University *2022*

Zhiyuan Honor Scholarship SJTU
Top 2% in SJTU *2018, 2019, 2020, 2021*

The 35nd China National Olympiad in Informatics CCF
Silver Medal *2017*

Projects

Qiling | *MCU, Python* [Link]

- Add MCU emulation module to the project, which can emulate MCUs from three top vendors.
- Add support for Cortex-M and RISCV architectures.
- Support fuzzing test of MCU firmware using afl.

Pymx | *Compiler, Python* [Link]

- Pymx is a compiler written in Python3 for compiling a Java-like language.
- Supports compile the source code into rv32im assembly code.
- Implemented many optimization methods, including global value numbering, dead code eliminate and SSA.
- The performance of the assembly code generated by the compiler is better than that generated by gcc with O1.

RV32-CPU | *FPGA, Verilog* [Link]

- This project is a RISC-V cpu with tomasulo algorithm implemented in Verilog HDL,
- The project works fine at 100M on the fpga and it did not show any errors during the experiment.
- Supports many useful features, include out-of-order execution, instruction cache, load buffer, etc.
- All the code of this project is original, not borrowed from any project.

Technical Skills

Languages: Chinese(Native), English(Fluent), Japnease(Knowledgeable)
Programming Languages: C, Python, C++, Rust, Javascript, Verilog
Frameworks: Angr, Unicorn, IDA, Qiling, Ghidra
Developer Tools: Git, VSCode, Emacs, Docker, Vivado, Android Studio
Hardware: STM32, Arduino, NXP, FPGA