Zheng Yu

zheng.yu@northwestern.edu | Personal Homepage

Education

Northwestern University Evanston, IL
Ph.D. Student, Computer Science Department *Sept 2022 - Present*

Shanghai Jiao Tong University Shanghai, China
Bachelor of Computer Science, Member of ACM Class *Sept 2018 - June 2022*

Yali High School Changsha, China
High School Student, focused on Algorithmic Competition *Sept 2015 - June 2018*

Experience

Project Mentor Apr 2022 – Oct 2022
Google Summer of Code 2022

- Mentored the Qiling Improvements projects.
- Provided guidance to developers on the project.

Software Security Engineer June 2021 – May 2022
JD.com, Inc. *JD Security*

- Member of the security team focusing on MCU firmware emulation.
- Core developer of Qiling, a binary analysis framework.

Research Assistant Feb 2021 – April 2021
Southern University of Science and Technology *Advised by: Yinqian Zhang*

- Worked on the design of remote attestation protocols for distributed TEE systems.
- Developed and improved the RISC-V trusted computing platform keystone-enclave.

Undergraduate Research Assistant July 2020 – June 2022
Sustainable Architectures and Infrastructure Laboratory (SAIL) *Advised by: Chao Li*

- Researched data center systems, architecture design, and cloud computing power management.
- Received high praise from Prof. Chao Li, noting my potential for graduate studies.

Website Operation Sept 2019 – Sept 2021
Network & Information Center, Shanghai Jiao Tong University

- Developed and maintained the Course Grade system for Zhiyuan College.
- Responsible for the maintenancex‘ of SJTU’s Online Judge platform.

Teaching Assistant June 2019 – Sept 2019
Programming Design Course (CS151), Shanghai Jiao Tong University

- Designed programming assignments and course projects.
- Recognized by students for my helpfulness and responsibility.

Publication

- GPTFUZZER: Red Teaming Large Language Models with Auto-Generated Jailbreak Prompts - *Jiahao Yu; Xinwei Lin;* ***Zheng Yu****; Xinyu Xing*

- CAMP: Compiler and Allocator-based Heap Memory Protection - *Zhenpeng Lin;* ***Zheng Yu****; Ziyi Guo; Simone Campanoni; Peter Dinda; Xinyu Xing* (USENIX Security 2024)

- FIRST: Exploiting the Multi-Dimensional Attributes of Functions for Power-Aware Serverless Computing - *Lu Zhang; Chao Li; Xinkai Wang; Weiqi Feng;* ***Zheng Yu****; Quan Chen; Jingwen Leng; Minyi Guo; Pu Yang; Shang Yue* (IPDPS 2023)

- Reversing MCU with Firmware Emulation - ***Zheng Yu****; KAI JERN LAU; MuChen Su; Anh Quynh NGUYEN* (BlackHat Europe 2022)

Academic Service

Journal Reviewer 2024
IEEE Transactions on Dependable and Secure Computing

Artifact Committee Member 2024
International Symposium on Software Testing and Analysis (ISSTA)

Artifact Committee Member 2024
USENIX Security Symposium (USENIX Security)

Program Committee Member 2024
International Conference on Edge Computing and IoT (ICECI)

Journal Reviewer 2023, 2024
High-Confidence Computing Journal

Artifact Committee Member 2023
ACM SIGSAC Conference on Computer and Communications Security (CCS)

Journal Reviewer 2023
PeerJ Computer Science Journal

Honors & Awards

5th at Defcon 23 CTF Finals DEFCON
StrawHat Team *2023*

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 (top 100) *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 elimination, 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)
Programming Languages: C/C++, SQL, Python, Java, Golang, Javascript, Rust, Verilog
Frameworks: MySQL, Redis, Hadoop, Spark, Angr, Unicorn, IDA, Qiling, Ghidra
Developer Tools: Git, VSCode, Emacs, Docker, Vivado, Android Studio
Hardware: STM32, Arduino, NXP, FPGA