Zheng Yu

zheng.yu@northwestern.edu

x

Education

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

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

Yali High School Hunan, China
High School Student, focused on Algorithmic Competition *Sep 2015 - June 2018*

Experience

Teaching Assistant Sep 2024 – Dec 2024
Introduction of Computer Security (COMP_SCI 350), Northwestern University

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

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

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

Undergraduate Research Assistant July 2020 – June 2022
SAIL Lab, Shanghai Jiao Tong University *Advised by: Chao Li*

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

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

Publication

- ShadowBound: Efficient Heap Memory Protection Through Advanced Metadata Management and Customized Compiler Optimization - ***Zheng Yu****; Ganxiang Yang; Xinyu Xing* (USENIX Security 2024)

- LLM-Fuzzer: Scaling Assessment of Large Language Model Jailbreaks - *Jiahao Yu; Xinwei Lin;* ***Zheng Yu****; Xinyu Xing* (USENIX Security 2024)

- 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

Program Committee Member 2025
International Conference on Machine Learning (ICML)

Program Committee Member 2025
International Conference on Learning Representations (ICLR)

Artifact Committee Member 2025
Network and Distributed System Security (NDSS)

Program Committee Member 2025
The Association for the Advancement of Artificial Intelligence Undergraduate Consortium (AAAI-UC)

Program Committee Member 2025
Artificial Intelligence and Statistics Conference (AISTATS)

Program Committee Member 2024
Conference on Neural Information Processing Systems (NeurIPS)

Journal Reviewer 2024
IEEE Transactions on Dependable and Secure Computing (TDSC)

Artifact Committee Member 2024
USENIX Annual Technical Conference (ATC)

Artifact Committee Member 2024
USENIX Symposium on Operating Systems Design and Implementation (OSDI)

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

Artifact Committee Member 2024, 2025
USENIX Security Symposium (USENIX Security)

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

Artifact Committee Member 2023, 2024
ACM SIGSAC Conference on Computer and Communications Security (CCS)

Journal Reviewer 2023, 2024
PeerJ Computer Science Journal

Honors & Awards

Advanced Final Competition at AICC Northwestern University
42-b3yond-6ug *2024*

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 35th China National Olympiad in Informatics CCF
Silver Medal (top 100) *2017*

Projects

Qiling | *MCU, Python* [Link]

- Integrated an MCU emulation module, capable of emulating microcontrollers from three leading vendors.
- Extended support for Cortex-M and RISC-V architectures.

Pymx | *Compiler, Python* [Link]

- Developed Pymx, a Python3-based compiler for a Java-like language.
- Compiles source code into RV32IM assembly language.

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

- Designed a RISC-V CPU with the Tomasulo algorithm implemented in Verilog HDL.
- Implemented features such as out-of-order execution, instruction cache, and load buffer.

Technical Skills

Languages: Chinese (Native), English (Fluent)
Programming Languages: C/C++, Python, Java, Javascript, Rust, Verilog
Frameworks: MySQL, Spark, Angr, Unicorn, IDA, Qiling, Ghidra
Developer Tools: Git, VSCode, Emacs, Docker, Vivado