Zheng Yu

zheng.yu@northwestern.edu | Homepage

Education

Northwestern University — Evanston, IL
Ph.D. Student, Computer Science Department, Advised by Xinyu Xing — *Sep 2022 - Present*
- Research Interests: AI Security, Software Security
- Focused on improving the security of software and AI systems.

Northwestern University — Evanston, IL
M.S. Student, Computer Science Department — *Sep 2022 - Dec 2024*

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

Visiting Researcher — Jun 2025 – Sept 2025
CrySp Lab, University of Waterloo — *Advised by: Meng Xu*

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

Security 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*

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

- PortGPT: Towards Automated Backporting Using Large Language Models - ***Zheng Yu****; Zhaoyang Li*; Jingyi Song; Meng Xu; Yuxuan Luo; Dongliang Mu* (IEEE S&P 2026)
- PatchAgent: A Practical Program Repair Agent Mimicking Human Expertise - ***Zheng Yu****; Ziyi Guo; Yuhang Wu; Jiahao Yu; Meng Xu; Dongliang Mu; Yan Chen; Xinyu Xing* (USENIX Security 2025)
- 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)

Talk & Speech

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

Honors & Awards

CSAW Applied Research Competition Finalist — NYU Tandon School of Engineering
PatchAgent — *2025*

USENIX Security Student Grant — USENIX
USENIX Security Symposium — *2024, 2025*

Advanced Final Competition at AIxCC — DARPA
42-b3yond-6ug — *2024*

CCS Student Grant — ACM SIGSAC
ACM CCS Conference — *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

PortGPT | *AI, Python* [Link]
- Developed PortGPT, an automated backporting tool leveraging large language models.
- Implemented novel techniques to enhance the accuracy and reliability of patch backporting.

PatchAgent | *Security, Python* [Link]
- Developed a program repair agent that mimics human expertise.
- Implemented a novel program repair algorithm based on large language models.

ShadowBound | *Security, C/C++* [Link]
- Developed a novel heap memory protection mechanism based on advanced metadata management.
- Implemented a customized compiler optimization to reduce runtime overhead.

GPT-Fuzzer | *AI, Python* [Link]
- Developed a fuzzer for large language models
- Implemented a novel method to scale the assessment of language model jailbreaks.

CAMP | *Security, C/C++* [Link]
- Developed a compiler and allocator-based heap memory protection mechanism.
- Implemented a novel compiler optimization to reduce runtime overhead.

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.

Academic Service

Program Committee Member 2025, 2026
International Conference on Learning Representations (ICLR)

Program Committee Member 2024, 2025
Conference on Neural Information Processing Systems (NeurIPS)

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

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

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

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

Artifact Committee Member 2023, 2024, 2025
ACM SIGSAC Conference on Computer and Communications Security (CCS)

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

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

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)

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

Journal Reviewer 2023, 2024
PeerJ Computer Science (PeerJ CS)

Technical Skills

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