Zheng Yu

zheng.yu@northwestern.edu | +1 312-520-5936

Education

Northwestern University — Chicago, IL, USA
Ph.D. Candidate in Computer Science (Advisor: Prof. Xinyu Xing) — *Sep 2022 – Expected Early 2026*

University of Waterloo — Waterloo, ON, Canada
Visiting Graduate Researcher — *Jun 2025 – Sep 2025*

Shanghai Jiao Tong University — Shanghai, China
Bachelor of Science in Computer Science | ACM Honors Program — *Sep 2018 – Jun 2022*

Core Competencies

High-Impact Open-Source Leadership

5,000+ Combined GitHub Stars | Industry & Government Recognition

- **Project Leadership:** Created GPT-Fuzzer (500+ stars), an LLM robustness testing framework integrated into Microsoft Azure's PyRIT security toolkit. Developed PatchAgent (100+ stars), an AI-powered automated program repair system that achieved DARPA AIxCC finalist status among 50+ international teams.
- **Core Maintainer Contributions:** Served as core developer for Qiling Framework (5,000+ stars), implementing hardware emulation modules. Contributed security patches and performance improvements to critical infrastructure projects including Linux Kernel, PHP interpreter, Assimp, GPAC, and Yasm assembler.
- **Competitive Programming Excellence:** Silver medalist at China National Olympiad in Informatics (NOI 2017), ranking top 100 among 10,000+ participants nationwide. Leveraged algorithmic expertise as Teaching Assistant for competitive programming and data structures courses at Shanghai Jiao Tong University.
- **Full-Stack Engineering:** Architected and deployed end-to-end systems across the technology stack. Expert proficiency in front-end technologies (JavaScript, React, CSS), back-end development (C/C++, Python, Java, Go, Rust), and cloud-native infrastructure (Docker, Kubernetes, CI/CD pipelines) for production-grade applications.

Pioneering Agentic System Design for Security Purpose

IEEE S&P & USENIX Security Publications | DARPA AIxCC Finalist

- **Patch Backporting Agent:** First-authored PortGPT, an LLM-based agent system for automated backporting with hierarchical workflow design to mitigate hallucination and context limitations. Published at IEEE S&P 2026 and backported 9 Linux kernel patches from mainline to stable versions, garnering coverage by tech media.
- **Automated Vulnerability Repair:** First-authored PatchAgent with innovative middleware layer between LLM and execution environment, enabling enhanced tool utilization. Accepted at USENIX Security 2025 and repaired 10 real-world CVEs across open-source projects including Pcapplusplus, libredwg, Assimp, libssh2, and HDF5.
- **End-to-End DARPA AIxCC System:** Core team member of 42-b3yond-6ug at DARPA AIxCC, architecting BugBuster—an LLM-powered system for automated vulnerability discovery and repair. Advanced to finalist position among 50+ international teams.

Deep Expertise in Low-Level Security & Systems

50+ CVE Discoveries | Compiler-Based Defenses | Highly-Cited AI Security Research

- **Compiler & Kernel Security:** First-authored ShadowBound and co-authored CAMP for userspace and kernel hardening, both published at USENIX Security. Implemented custom LLVM optimization passes, showing mastery of compiler and low-level memory management across privilege boundaries.
- **Vulnerability & Exploit Study:** Discovered 50+ CVEs across userspace applications and the Linux kernel through systematic security analysis. Top 5 finalist at DEFCON CTF Finals (2022-2023) with team StrawHat, showcasing deep understanding of binary exploitation and defense mechanisms.
- **AI Security Research Impact:** Co-authored GPT-Fuzzer (published as LLM-Fuzzer at USENIX Security 2024), which has become a foundational work in LLM jailbreak assessment. The framework was integrated into Microsoft Azure's PyRIT security toolkit.

Publications

** denotes equal contribution*

PortGPT: Towards Automated Backporting Using Large Language Models
Zheng Yu*, *Zhaoyang Li**, *Jingyi Song, Meng Xu, Yuxuan Luo, Dongliang Mu*
IEEE Symposium on Security and Privacy (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 Symposium 2025

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

LLM-Fuzzer: Scaling Assessment of Large Language Model Jailbreaks
Jiahao Yu, Xingwei Lin, ***Zheng Yu****, Xinyu Xing*
USENIX Security Symposium 2024

CAMP: Compiler and Allocator-based Heap Memory Protection
Zhenpeng Lin, ***Zheng Yu****, Ziyi Guo, Simone Campanoni, Peter Dinda, Xinyu Xing*
USENIX Security Symposium 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*
IEEE International Parallel and Distributed Processing Symposium (IPDPS) 2023

Teaching Experience

Operating Systems (COMP_SCI 343) Sep 2025 – Dec 2025
Graduate Teaching Assistant, Northwestern University *Instructor: Dr. Branden Ghena*

Introduction to Computer Security (COMP_SCI 350) Sep 2024 – Dec 2024
Graduate Teaching Assistant, Northwestern University *Instructor: Prof. Xinyu Xing*

Programming Design and Data Structures (CS151) Jun 2019 – Sep 2019
Undergraduate Teaching Assistant, Shanghai Jiao Tong University *Instructor: Prof. Huiyu Weng*

Professional Experience

Google Summer of Code (Part-time) Remote
Project Mentor – Qiling Framework *Apr 2022 – Oct 2022*

- Mentored international contributors on MCU emulation and firmware analysis implementations.
- Guided development of RISC-V and Cortex-M architecture support for the Qiling emulation framework.

JD.COM, Inc. Beijing, China
Security Engineer – Application Security Team *Jun 2021 – May 2022*

- Conducted vulnerability research and security assessments for large-scale e-commerce infrastructure.
- Developed automated security testing tools and contributed to internal security training programs.

Shanghai Jiao Tong University Shanghai, China
Infrastructure Engineer – Information and Network Center *Sep 2019 – May 2021*

- Maintained and optimized university-wide computing infrastructure serving 40,000+ users.
- Implemented monitoring solutions and performance improvements for critical campus systems.

Selected Projects

PortGPT | *LLM-based Automated Patch Backporting* [GitHub]

- Engineered an LLM-powered system for automatically backporting security patches across software versions, addressing a critical challenge in software maintenance that traditionally requires significant manual expert effort.
- Implemented novel prompt engineering techniques and validation mechanisms to ensure backport correctness.

PatchAgent | *AI-Powered Program Repair System* [GitHub]

- Built an intelligent program repair agent that mimics human debugging workflows using large language models, achieving state-of-the-art performance on standard benchmarks and recognition as a DARPA AIxCC finalist.
- Designed multi-stage repair pipeline incorporating static analysis, dynamic testing, and iterative refinement.

ShadowBound | *Compiler-Based Memory Safety* [GitHub]

- Developed novel heap memory protection mechanism using advanced metadata management and LLVM-based compiler optimizations, achieving significant performance improvements over existing solutions.
- Implemented custom LLVM passes for fine-grained memory instrumentation with minimal runtime overhead.

GPT-Fuzzer | *LLM Security Testing Framework* [GitHub]

- Created scalable fuzzing infrastructure for evaluating LLM safety properties and jailbreak resistance, now integrated into Microsoft Azure's PyRIT security toolkit used by enterprise customers worldwide.
- Pioneered template-based generation techniques for systematic exploration of prompt injection vulnerabilities.

Qiling Framework | *Advanced Binary Emulation* [GitHub]

- Core contributor to multi-platform binary emulation framework with 5,000+ GitHub stars. Implemented comprehensive MCU emulation module supporting STM32, GigaDevice, and SiFive microcontrollers across ARM Cortex-M and RISC-V architectures.
- Extended firmware analysis capabilities and integrated AFL fuzzing support for embedded systems testing.

Pymx Compiler | *Educational Compiler Infrastructure* [GitHub]

- Designed and implemented a complete compiler for Java-like language targeting RISC-V architecture, featuring lexical analysis, parsing, semantic analysis, optimization passes, and code generation to RV32IM assembly.

RISC-V CPU Implementation | *Hardware Design* [GitHub]

- Architected RISC-V processor in Verilog HDL implementing Tomasulo algorithm for out-of-order execution, with instruction cache, load buffer, and branch prediction for enhanced performance on FPGA platforms.

Honors & Awards

CSAW Applied Research Competition Finalist 2025
NYU Tandon School of Engineering – PatchAgent Project

USENIX Security Student Grant Recipient 2024, 2025
USENIX Association

DARPA AIxCC Advanced Finals 2024
Top Finalist – Team 42-b3yond-6ug

ACM CCS Student Grant Recipient 2024
ACM SIGSAC Conference on Computer and Communications Security

DEFCON CTF Finals – 5th Place 2023
Team StrawHat (7th Place in 2022)

Outstanding Graduate Award 2022
Shanghai Jiao Tong University

Zhiyuan Honor Scholarship 2018–2021
Shanghai Jiao Tong University (Top 2% annually)

China National Olympiad in Informatics – Silver Medal 2017
China Computer Federation (CCF) – Top 100 Nationally

Conference Presentations

Reversing MCU with Firmware Emulation Dec 2022
BlackHat Europe *London, UK*

Academic Service

Program Committee Member
AI/ML Conferences

- International Conference on Learning Representations (ICLR) – 2025, 2026
- Conference on Neural Information Processing Systems (NeurIPS) – 2024, 2025
- International Conference on Machine Learning (ICML) – 2025
- Artificial Intelligence and Statistics (AISTATS) – 2025
- AAAI Undergraduate Consortium (AAAI-UC) – 2025

Artifact Evaluation Committee Member
Security & Systems Conferences

- ACM Conference on Computer and Communications Security (CCS) – 2023, 2024, 2025
- USENIX Security Symposium – 2024, 2025
- Network and Distributed System Security Symposium (NDSS) – 2025
- USENIX Annual Technical Conference (ATC) – 2024
- Operating Systems Design and Implementation (OSDI) – 2024
- International Symposium on Software Testing and Analysis (ISSTA) – 2024

Peer Reviewer
Academic Journals

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- PeerJ Computer Science

Technical Skills

Programming Languages: C/C++ (Expert), Python (Expert), Rust, Java, JavaScript/TypeScript, Go, OCaml, Verilog HDL
Security & Binary Analysis: IDA Pro, Ghidra, Angr, Unicorn Engine, Qiling Framework, Binary Ninja, GDB
AI/ML Frameworks: PyTorch, LangChain, Transformers, OpenAI API, Anthropic API
Systems & Compilers: LLVM/Clang, GCC, Linux Kernel Development, QEMU, Unicorn
Development Tools: Git, Docker, Kubernetes, CI/CD (GitHub Actions, Jenkins), Vivado, VSCode, Emacs
Databases & Infrastructure: MySQL, PostgreSQL, Redis, Apache Spark, Elasticsearch
Languages: English (Fluent), Chinese (Native)