

# Zheng Yu

[zheng.yu@northwestern.edu](mailto:zheng.yu@northwestern.edu) | [Homepage](#)

## EDUCATION

### Northwestern University

*Ph.D. Student, Computer Science Department, Advised by Xinyu Xing*

- Research Interests: AI Security, Software Security
- Focused on improving the security of software and AI systems.

Evanston, IL

Sep 2022 - Present

### Northwestern University

*M.S. Student, Computer Science Department*

Evanston, IL

Sep 2022 - Dec 2024

### Shanghai Jiao Tong University

*Bachelor of Computer Science, Member of ACM Class*

Shanghai, China

Sep 2018 - June 2022

### Yali High School

*High School Student, focused on Algorithmic Competition*

Hunan, China

Sep 2015 - June 2018

## EXPERIENCE

### Visiting Researcher

*CrySp Lab, University of Waterloo*

Jun 2025 – Sept 2025

*Advised by: Meng Xu*

### Teaching Assistant

*Introduction of Computer Security (COMP\_SCI 350), Northwestern University*

Sep 2024 – Dec 2024

### Project Mentor

*Summer of Code 2022, Google*

Apr 2022 – Oct 2022

### Security Engineer

*JD.com, Inc.*

June 2021 – May 2022

### Research Assistant

*RITAS Lab, Southern University of Science and Technology*

Feb 2021 – April 2021

*Advised by: Yinqian Zhang*

### Research Assistant

*SAIL Lab, Shanghai Jiao Tong University*

July 2020 – June 2022

*Advised by: Chao Li*

### Website Operation

*Network & Information Center, Shanghai Jiao Tong University*

Sep 2019 – Sep 2021

### Teaching Assistant

*Programming Design Course (CS151), Shanghai Jiao Tong University*

June 2019 – Sep 2019

## 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

---

<b>Advanced Final Competition at AICC</b> <i>42-b3yond-6ug</i>	Northwestern University 2024
<b>5th at Defcon 23 CTF Finals</b> <i>StrawHat Team</i>	DEFCON 2023
<b>7th at Defcon 22 CTF Finals</b> <i>StrawHat Team</i>	DEFCON 2022
<b>Outstanding Graduates</b> <i>Outstanding Graduate of Shanghai Jiaotong University</i>	SJTU 2022
<b>Zhiyuan Honor Scholarship</b> <i>Top 2% in SJTU</i>	SJTU 2018, 2019, 2020, 2021
<b>The 35th China National Olympiad in Informatics</b> <i>Silver Medal (top 100)</i>	CCF 2017

## PROJECTS

---

<b>PatchAgent</b>   <i>Security, Python</i> <ul style="list-style-type: none"><li>• Developed a program repair agent that mimics human expertise.</li><li>• Implemented a novel program repair algorithm based on large language models.</li></ul>	<a href="#">[Link]</a>
<b>ShadowBound</b>   <i>Security, C/C++</i> <ul style="list-style-type: none"><li>• Developed a novel heap memory protection mechanism based on advanced metadata management.</li><li>• Implemented a customized compiler optimization to reduce runtime overhead.</li></ul>	<a href="#">[Link]</a>
<b>GPT-Fuzzer</b>   <i>AI, Python</i> <ul style="list-style-type: none"><li>• Developed a fuzzer for large language models</li><li>• Implemented a novel method to scale the assessment of language model jailbreaks.</li></ul>	<a href="#">[Link]</a>
<b>CAMP</b>   <i>Security, C/C++</i> <ul style="list-style-type: none"><li>• Developed a compiler and allocator-based heap memory protection mechanism.</li><li>• Implemented a novel compiler optimization to reduce runtime overhead.</li></ul>	<a href="#">[Link]</a>
<b>Qiling</b>   <i>MCU, Python</i> <ul style="list-style-type: none"><li>• Integrated an MCU emulation module, capable of emulating microcontrollers from three leading vendors.</li><li>• Extended support for Cortex-M and RISC-V architectures.</li></ul>	<a href="#">[Link]</a>
<b>Pymx</b>   <i>Compiler, Python</i> <ul style="list-style-type: none"><li>• Developed Pymx, a Python3-based compiler for a Java-like language.</li><li>• Compiles source code into RV32IM assembly language.</li></ul>	<a href="#">[Link]</a>
<b>RV32-CPU</b>   <i>FPGA, Verilog</i> <ul style="list-style-type: none"><li>• Designed a RISC-V CPU with the Tomasulo algorithm implemented in Verilog HDL.</li><li>• Implemented features such as out-of-order execution, instruction cache, and load buffer.</li></ul>	<a href="#">[Link]</a>

## ACADEMIC SERVICE

---

<b>Program Committee Member</b> <i>International Conference on Machine Learning (ICML)</i>	2025
<b>Program Committee Member</b> <i>International Conference on Learning Representations (ICLR)</i>	2025
<b>Artifact Committee Member</b> <i>Network and Distributed System Security (NDSS)</i>	2025
<b>Program Committee Member</b> <i>The Association for the Advancement of Artificial Intelligence Undergraduate Consortium (AAAI-UC)</i>	2025
<b>Program Committee Member</b> <i>Artificial Intelligence and Statistics Conference (AISTATS)</i>	2025
<b>Program Committee Member</b> <i>Conference on Neural Information Processing Systems (NeurIPS)</i>	2024
<b>Journal Reviewer</b> <i>IEEE Transactions on Dependable and Secure Computing (TDSC)</i>	2024
<b>Artifact Committee Member</b> <i>USENIX Annual Technical Conference (ATC)</i>	2024
<b>Artifact Committee Member</b> <i>USENIX Symposium on Operating Systems Design and Implementation (OSDI)</i>	2024
<b>Artifact Committee Member</b> <i>International Symposium on Software Testing and Analysis (ISSTA)</i>	2024
<b>Artifact Committee Member</b> <i>USENIX Security Symposium (USENIX Security)</i>	2024, 2025
<b>Artifact Committee Member</b> <i>ACM SIGSAC Conference on Computer and Communications Security (CCS)</i>	2023, 2024
<b>Journal Reviewer</b> <i>PeerJ Computer Science Journal</i>	2023, 2024

## 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