ZIYI(ROLAND) GUO

ziyi.guo@northwestern.edu ◇ HomePage

EDUCATION

Northwestern University 2023 -
Ph.D. Student in Computer Science with Prof.Yan Chen, Prof.Xinyu Xing

Sichuan University 2019 - 2023
Cyber Security, B.E.

WORK EXPERIENCE

S&P Group, Northwestern University 2022 -
Research Assistant, work on Vulnerability Analysis, Exploitation, Defense; Program Repair.

NISL, Tsinghua University 2022 - 2023
Research Assistant, work on eBPF-based attacks in Cloud System.

Xuanwu Lab, Tencent 2021 - 2022
Security Researcher, work on Cloud System and Linux Kernel Vulnerability Exploitation

RESEARCH INTERESTS

Software and System Security; Large Language Models(LLMs) for Security

PUBLICATIONS AND MANUSCRIPTS

Take a Step Further: Understanding Page Spray in Linux Kernel Exploitation.
33rd USENIX Security Symposium(USENIX Security) 2024
Ziyi Guo, Dang K Le, Zhenpeng Lin, Kyle Zeng, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, Adam Doupé, Xinyu Xing
TL;DR: From heap level attack to page level attack.

CAMP: Compiler and Allocator-based Heap Memory Protection.
33rd USENIX Security Symposium(USENIX Security) 2024
Zhenpeng Lin, Zheng Yu, **Ziyi Guo**, Simone Campanoni, Peter Dinda, Xinyu Xing
TL;DR: Compiler and allocator co-design to protect programs.

Cross Container Attacks: The Bewildered eBPF on Clouds.
32nd USENIX Security Symposium(USENIX Security) 2023
Yi He* and **Roland Guo***(co-first author), Yunlong Xing, Xijia Che, Kun Sun, Zhuotao Liu, Ke Xu, Qi Li
TL;DR: eBPF-based attacks in cloud system.

Guiding Large Language Models to Repair Real World Vulnerabilities
Under Review
TL;DR: Design and implement LLMs-enhanced system to repair realworld vulnerabilities.

COMPETITION

- Winner, DARPA's AIxCC Semi-Final. Core member of Team 42-b3yond-6ug, awarded $2 Million, 08/2024. **[DARPA News Link]**
- Top 7 in the world, DARPA's AIxCC Purposal and Design. Core member of Team 42-b3yond-6ug, funded $1 Million, 03/2024. **[DARPA News Link]**
- World Finalist, DEF CON CTF, Team r3kapig, 08/2022.
- World Finalist, DEF CON CTF, Team r3kapig, 08/2021.

ACADEMIC SERVICES

Artifact Evaluation Committee(AEC) Member: USENIX Security 2024, ISSTA 2024.
External Reviewer: IEEE S&P 2024, IEEE S&P 2025.