Roland Ziyi Guo

E-Mail, GoogleScholar

EDUCATION

Northwestern University, Evanston, IL, USA Sep 2023 – Present

- Ph.D. Student in Computer Science

Sichuan University, Chengdu, Sichuan, China Sep 2019 – Aug 2023

- B.E. in Cyber Science.

RESEARCH INTERESTS

Systems and Software Security

- Security Problems in Operating Systems, Cloud Systems, Blockchain Infra and etc...
- Vulnerability and Bugs Security Analysis, Exploitation, Mitigation, and Defense.

LLMs for Systems and Software Security

- Apply LLMs to solve security problems, and improve security for system.

PUBLICATIONS

[Link] Ziyi Guo, Dang K Le, Zhenpeng Lin, Kyle Zeng, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, Adam Doupé, Xinyu Xing, "*Take a Step Further: Understanding Page Spray in Linux Kernel Exploitation* ," in **USENIX Security 2024**

[Link] Zhenpeng Lin, Zheng Yu, Ziyi Guo, Simone Campanoni, Peter Dinda, Xinyu Xing, "*CAMP: Compiler and Allocation-based Memory Protection*," in **USENIX Security 2024**

[Link] Yi He* and Roland Guo***(Co-first author)**, Yunlong Xing, Xijia Che, Kun Sun, Zhuotao Liu, Ke Xu, Qi Li, "*Cross Container Attacks: The Bewildered eBPF on Clouds*," in **USENIX Security 2023**

DRAFTS

"*One paper about Large Language Models(LLMs) for Program Repair* ," **Under Review**

"*One paper about Webassembly(WASM) Fuzzing* ," **Under Review**

WORK EXPERIENCE

Tencent Security Xuanwu Lab

- Security Researcher Oct 2021 – Mar 2022
  - Research Topics: (1) Kernel Security; (2) Cloud System Security
  - Focus: Explore the methods to corrupt cloud system by Linux Kernel Vulnerability; Explore the offensive features(i.e. eBPF) in Linux Kernel which threats the cloud system.

COMPETITION

- World Finalist, Team r3kapig, DEF CON CTF 2021,2022
- 5th Place, Team 42-b3yond-6ug, DARPA AI Cybersecurity Challenge(AIxCC) [Link] 2024

COMMUNITY SERVICE

Program Committee in AE
USENIX Security 2024, ISSTA 2024
External Reviewer
IEEE S&P(”Okaland”) 2024, IEEE S&P(”Okaland”) 2025

SKILLS

LaTeX, Vulnerability Exploitation, Kernel Programming, eBPF Programming,
Fuzzing, Reverse Engineering, Underlying System Debugging, LLVM-Based Program Analysis.