MUQI ZOU

zou116@purdue.edu

Education

Purdue University West Lafayette, IN, US

Ph.D. candidate in Computer Science, Aug 2018 – expected Dec 2025

Advisors: Prof. Dongyan Xu and Prof. Ruoyu Wang

University of Illinois at Urbana-Champaign Urbana-Champaign, IL, US

B.S. in Computer Science Aug 2013 - May 2016

Xi'an Jiaotong-Liverpool University Suzhou, China

B.S. in Electrical Engineering Aug 2011 - May 2013

Experience

FRIENDS Lab and PURSEC Lab West Lafayette, IN, US

Graduate Research Assistant Aug 2020 – Current

- Built an automatic framework at the IR (e.g., LLVM, P-Code) level for verifying the code semantics and binary behavior using symbolic execution and SMT solvers.
- Developed an automated decompiler backend that harnesses and fine-tunes LLMs with reinforcement learning (GRPO) to improve decompilation quality.
- Developed an automated decompiler debugging system to identify and localize root causes of bugs, enhancing the reliability of state-of-the-art decompilers.
- Helped develop a dynamic analysis framework for reverse engineering Deep Neural Networks (DNNs) on edge devices.
- Helped test an obfuscation system to defend DNN models against reverse-engineering attacks.
- Helped extend AFLplusplus to create a program mutation-based fuzzer, which enables Intel SGX enclave fuzzing on commodity machines.
- Helped implement a framework using LLM for cyber threat intelligence mapping and response.

Purdue University West Lafayette, IN, US

Graduate Teaching Assistant Aug 2019 - May 2020

- CS354 Operating Systems (Spring 2020) — Grading and office hours.
- CS503 Operating Systems (Fall 2019) — Grading, office hours, designed and implemented a homework project.

Publications

Peer-reviewed conference publications:

C1. **Muqi Zou**, Hongyu Cai, Hongwei Wu, Zion Leonahenahe Basque, Arslan Khan, Berkay Celik, Dave (Jing)Tian, Antonio Bianchi, Ruoyu (Fish)Wang, and Dongyan Xu. "D-LiFT: Improving LLM-based Decompiler Backend via Code Quality-driven Fine-tuning." arXiv preprint, https://arxiv.org/abs/2506.10125

C2. Solomon Sonya, **Muqi Zou**, Saastha Vasan, Christopher Kruegel, Giovanni Vigna and Dongyan Xu. “One Size Doesn’t Fit All: A Dynamic Heterogeneous Learning Ensemble for Malware Family Classification.” Workshop on Security and AI in conjunction with ESORICS (SECAI’25), 2025

C3. Zheng Zhong, Ruoyu Wu, Junpeng Wan, **Muqi Zou**, and Dave (Jing) Tian. “Hardening Deep Neural Network Binaries against Reverse Engineering Attack.” 32nd ACM Conference on Computer and Communications Security (CCS’25), 2025.

C4. Ruoyu Wu, **Muqi Zou**, Arslan Khan, Taegyu Kim, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. “NeuroScope: Reverse Engineering Deep Neural Network on Edge Devices using Dynamic Analysis.” 34th USENIX Security Symposium (USENIX Security’25), 2025.

C5. **Muqi Zou**, Arslan Khan, Ruoyu Wu, Han Gao, Antonio Bianchi, and Dave (Jing) Tian. “D-Helix: A Generic Decompiler Testing Framework Using Symbolic Differentiation.” 33rd USENIX Security Symposium (USENIX Security’24), 2024.

C6. Arslan Khan, **Muqi Zou**, Kyungtae Kim, Dongyan Xu, Antonio Bianchi, and Dave Jing Tian. “Fuzzing SGX Enclaves via Host Program Mutations.” 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P’23), 2023.