MUQI ZOU

zou116@purdue.edu

Education

Purdue University West Lafayette, IN, US

Ph.D. candidate in Computer Science, Aug 2020 – expected Dec 2025

Advisors: Prof. Dongyan Xu and Prof. Ruoyu Wang

Purdue University West Lafayette, IN, US

M.S. in Computer Science Aug 2018 - May 2020

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

- Developed an automated decompiler backend that harnesses and fine-tunes LLMs with reinforcement learning to improve decompilation quality.
- Built an automatic framework for debugging decompilers using symbolic execution and SMT solvers.
- Helped develop a dynamic analysis framework for reverse engineering Deep Neural Networks (DNNs) on edge devices.
- Helped test a 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.

Purdue University West Lafayette, IN, US

Graduate Teaching Assistant Sep 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.*** Under submission.

C2. 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), 2025.

C3. 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 (Security'25), 2025.

C4. **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 (Security'24), 2024.

C5. 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), 2023.