Shixuan Zhao

Email: shixuan.zhao@hotmail.com

Homepage: https://nskernel.org

HIGER EDUCATION

BS (Elite Class): 09/2016 – 07/2020

GPA: 4.43/5.0

Nanjing University, Computer Science and Technology — Nanjing, Jiangsu, P.R.China

PhD Candidate: 01/2022 – 12/2025 (estimated)

GPA: 4.0/4.0

The Ohio State University, Computer Science and Engineering — Columbus, OH, USA

RESEARCH & PUBLICATIONS

GPU Travelling: Efficient Confidential Collaborative Training with TEE-Enabled GPUs

Shixuan Zhao, Zhongshu Gu, Salman Ahmed, Enriquillo Valdez, Hani Jamjoom, Zhiqiang Lin

Top-Tier Conference ACM CCS 2025 (Under Minor Revision). US Patent pending.

Dramatically improved performance confidential collaborative ML workloads by letting GPUs to switch to and directly collect dataset from data holder confidential VMs while maintaining dataset confidentiality.

Ditto: Elastic Confidential VMs with Secure and Dynamic CPU Scaling

Shixuan Zhao, Mengyuan Li, Mengjia Yan and Zhiqiang Lin

arXiv Preprint. Under submission.

Allows dynamic vCPU scaling for confidential VMs on the fly with a demonstration application to confidential serverless.

Deanonymizing Device Identities via Side-Channel Attacks in Exclusive-use IoTs & Mitigation

Christopher Ellis, Yue Zhang, Mohit Kumar Jangid, **Shixuan Zhao** and Zhiqiang Lin

Top-Tier Conference NDSS 2025

Proposed a side-channel attack for wireless communications like BLE and Wi-Fi that can cause identity and privacy leakage. Designed a protocol-level mitigation of this attack.

STYX: Collaborative and Private Data Processing With TEE-Enforced Sticky Policy

Shixuan Zhao, Weiching Wang, Ninghui Li and Zhiqiang Lin

Under submission.

Designed a TEE-based sticky policy middleware that can sandbox arbitrary code to work on confidential data while enforcing a programmable policy support even on derived data.

Reusable Enclaves for Confidential Serverless Computing

Shixuan Zhao, Pinshen Xu, Guoxing Chen, Mengya Zhang, Yinqian Zhang and Zhiqiang Lin

Top-Tier Conference USENIX Security 2023

Solves cold start problem in confidential serverless computing by enabling an enclave to be reset to its initial state so the booting overhead can be eliminated.

vSGX: Virtualizing SGX Enclaves on AMD SEV

Shixuan Zhao, Mengyuan Li, Yinqian Zhang and Zhiqiang Lin

Top-Tier Conference IEEE S&P 2022

Allows to run Intel SGX apps with binary compatibility and a comparable security on AMD SEV.

Read-Copy Update (RCU) Bug Auto Detection in Linux Kernel

Independently conducted project. Supervised by Prof. Yanyan Jiang

This research aims to find the common cause for RCU bugs, automatically test system calls related to RCU and seek for how to reproduce bugs when they occur.

A GUI Based Dynamic Birthmark Generation Method for Android Applications

A National Innovation project. Concluded with honour.

Leader. Supervised by Prof. Jun Ma

PATENT

- Nanjing University. A Detection Method for Repackaged Android Applications Based on Interface Icon Features: China, CN109815699B, 2018-12-15.
- IBM. Traveling Hardware Accelerator for Data Sharing in Collaborative Learning. US. Pending.

HONOURS

- Scholarship for Elite Training Program, NJU, 12/2017 and 12/2018
- Scholarship for Excellent Freshman, NJU, 12/2016
- Suning Elite Fellowship, NJU & Suning Holdings Group Co., Ltd. (16 out of 2000), 09/2016

EXPERIENCES

- Research Assistant. Southern University of Science and Technologies. 03/2021 – 09/2021
- Graduate Research/Teaching Assistant. The Ohio State University. 01/2022 – Present
- Research Scientist Intern – Security Pillar. IBM Research. 05/2024 – 08/2024
- Research Scientist Intern – Security Research Group. Microsoft Research. 05/2025 – 08/2025

SERVICES

- EAI International Conference on Edge Computing and IoT 2024 (ICECI'24), TPC Member
- EAI SecureComm 2022, Reviewer
- ACM Transactions on Privacy and Security, Reviewer
- IEEE Internet of Things Journal, Reviewer
- IEEE S&P 2021-2025 Reviewer
- USENIX Security 2021-2024, Reviewer
- USENIX Security 2025, Artefact Review Committee Member
- ACM CCS 2021-2024, Reviewer