Ziqi Zhang

Gender: Male · Age: 30 · Email: ziqi.zhang25@gmail.com · 🔗 https://ziqi-zhang.github.io

Research Interest

Research interests: Software engineering, LLM agent security, hardware security
Research goal: Building a reliable and secure platform for LLM agent.

- LLM Agent for Cybersecurity (NeurIPS25)
- TEE-based Secure Agent Platform (NeurIPS25, Security25, S&P24, TOSEM25, ICML24,ISSTA22W)
- Software Engineering for AI (ESEC/FSE20, ICSE22, ISSTA21)
- AI Privacy and Security (ICSE23, Ubicomp22, WWW23, Security24, Security25, Ubicomp25, S&P25, S&P26, EMNLP25)

Employment

University of Illinois Urbana-Champaign, IL, US 2024.03 – present
PostDoc in Computer Science. Mentor: Prof. Lingming Zhang

Peking University, Beijing, China 2023.07 – 2024.02
PostDoc in Computer Software and Theory. Mentor: Prof. Yao Guo

Education

Peking University, Beijing, China 2018.09 – 2023.07
Ph.D. in Computer Software and Theory
Advisers: Prof. Ding Li, Prof. Yao Guo, and Prof. Xiangqun Chen

Peking University, Beijing, China 2014.09 – 2018.07
B.S. in Computer Science

Selected Publications

Note: * represents co-first author, † indicates corresponding author.

- **[NeurIPS 2025]** Hwiwon Lee, **Ziqi Zhang**, Hanxiao Lu, Lingming Zhang. ”SEC-bench: Automated Benchmarking of LLM Agents on Real-World Software Security Tasks”
- **[USENIX Security 2025]** Pengli Wang, Bingyou Dong, Yifeng Cai, Zheng Zhang, Junlin Liu, Huanran Xue, Ye Wu, Yao Zhang, and **Ziqi Zhang**†. ”Game of Arrows: On the (In-)Security of Weight Obfuscation for On-Device TEE-Shielded LLM Partition Algorithms”. In Proceedings of the 2025 USENIX Security Symposium.
- **[TOSEM 2025]** Ding Li, **Ziqi Zhang**†, Mengyu Yao, Yifeng Cai, Yao Guo, and Xiangqun Chen. ”TEESlice: Protecting Sensitive Neural Network Models in Trusted Execution Environments When Attackers have Pre-Trained Models”. ACM Transactions on Software Engineering and Methodology.
- **[S&P 2024] Ziqi Zhang**, Chen Gong, Yuanyuan Yuan, Yifeng Cai, Bingyan Liu, Ding Li, Yao Guo, Xiangqun Chen. ”No Privacy Left Outside: On the (In-)Security of TEE-Shielded DNN Partition Defenses”. In 2024 IEEE Symposium on Security and Privacy (SP).
- **[ICSE 2023] Ziqi Zhang**, Yuanchun Li, Bingyan Liu, Yifeng Cai, Ding Li, Yao Guo, Xiangqun Chen. ”FedSlice: Protecting Federated Learning Models from Malicious Participants with Model Slicing”. In Proceedings of the 45th International Conference on Software Engineering.
- **[ICSE 2022] Ziqi Zhang**, Yuanchun Li, Jindong Wang, Bingyan Liu, Ding Li, Xiangqun Chen, Yao Guo, Yunxin Liu. ”ReMoS: Reducing Defect Inheritance in Transfer Learning via Relevant Model Slicing”. In Proceedings of the 44th International Conference on Software Engineering.
- **[ESEC/FSE 2020] Ziqi Zhang**, Yuanchun Li, Yao Guo, Xiangqun Chen, Yunxin Liu. ”Dynamic Slicing for Deep Neural Networks.” In 2020 ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering.

Other Publications

- **[S&P 2026]** Shaofei Li, **Ziqi Zhang**, Xiao Han, Zhenkai Liang, Yao Guo, Xiangqun Chen, Ding Li, Shuli Gao, Minyao Hua. ”PromoGuardian: Detecting Promotion Abuse Fraud with Multi-Relation Fused Graph Neural Networks” In 2026 IEEE Symposium on Security and Privacy (SP).
- **[EMNLP 2025]** **Ziqi Zhang**, Ali Shahin Shamsabadi, Hanxiao Lu, Yifeng Cai, Hamed Haddadi. ”Membership and Memorization in LLM Knowledge Distillation”
- **[NeurIPS 2025]** Che Wang, **Ziqi Zhang**†, Yinggui Wang, Tiantong Wang, Yurong Hao, Jianbo Gao, Tao Wei, Yang Cao, Zhong Chen, Wei Yang Bryan Lim. ”AegisGuard: RL-Guided Adapter Tuning for TEE-Based Efficient Secure On-Device Inference” In Proceedings of the 39th Conference on Neural Information Processing Systems.
- **[USENIX Security 2025]** Yifeng Cai, **Ziqi Zhang**†, Mengyu Yao, Junlin Liu, Xiaoke Zhao, Xinyi Fu, Ruoyu Li, Zhe Li, Ding Li†, Yao Guo, Xiangqun Chen. ”I Can Tell Your Secrets: Inferring Privacy Attributes from Mini-app Interaction History in Super-apps” In Proceedings of the 2025 USENIX Security Symposium.
- **[Ubicomp 2025]** Yifeng Cai, **Ziqi Zhang**, Ding Li, Yao Guo, and Xiangqun Chen. ”MOSS: Proxy Model-based Full-Weight Aggregation in Federated Learning with Heterogeneous Models” In Proceedings of the 2025 ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.
- **[S&P 2025]** Shaofei Li, **Ziqi Zhang**†, Haoming Jia, Yao Guo, Xiangqun Chen, Ding Li†. ”Query Provenance Analysis: Efficient and Robust Defense against Query-based Black-box Attacks” In 2025 IEEE Symposium on Security and Privacy (SP).
- **[RTSS 2024]** Zhaomeng Deng, **Ziqi Zhang**, Yao Guo, Yunfeng Ye, Yuxin Ren, Ning Jia, Xinwei Hu, Ding Li. ”Interference-free Operating System: A 6 Years’ Experience in Mitigating Cross-Core Interference in Linux” In Proceedings of the 2024 IEEE Real-Time Systems Symposium.
- **[USENIX Security 2024]** Yifeng Cai*, **Ziqi Zhang***, Jiaping Gui, Bingyan Liu, Xiaoke Zhao, Ruoyu Li, Zhe Li, Ding Li. ”FAMOS: Robust Privacy-Preserving Authentication on Payment Apps via Federated Multi-Modal Contrastive Learning” In Proceedings of the 2024 USENIX Security Symposium.
- **[ICML 2025]** Zheng Zhang, Na Wang, **Ziqi Zhang**, Tianyi Zhang, Jianwei Liu, Yao Zhang, Ye Wu. ”GroupCover: A Secure, Efficient and Scalable Inference Framework for On-device Model Protection based on TEEs” In Proceedings of the 41st International Conference on Machine Learning.
- **[ISSRE 2023]** Shaokun Zhang, Wu Linna, Yuanchun Li, **Ziqi Zhang**, Hanwei Lei, Ding Li, Yao Guo, and Xiangqun Chen. ”ReSPlay: Improving Cross-Platform Record-and-Replay with GUI Sequence Matching”. In Proceedings of the 2023 IEEE International Symposium on Software Reliability Engineering.
- **[CCS 2023]** Yuanpeng Wang, **Ziqi Zhang**, Ningyu He, Zhineng Zhong, Shengjian Guo, Qinkun Bao, Ding Li, Yao Guo, and Xiangqun Chen. ”SymGX: Detecting Cross-boundary Pointer Vulnerabilities of SGX Applications via Static Symbolic Execution”, In Proceedings of the 2023 ACM Conference on Computer and Communications Security.
- **[CCS 2023]** Hanwen Lei, **Ziqi Zhang**, Shaokun Zhang, Peng Jiang, Zhineng Zhong, Ningyu He, Ding Li, Yao Guo, and Xiangqun Chen. ”Put Your Memory in Order: Efficient Domain-based Memory Isolation for WASM Applications”, In Proceedings of the 2023 ACM Conference on Computer and Communications Security.
- **[WWW 2023]** Bingyan Liu, Yifeng Cai, Hongzhe Bi, **Ziqi Zhang**, Ding Li, Yao Guo, Xiangqun Chen. ”Beyond Fine-Tuning: Efficient and Effective Fed-Tuning for Mobile/Web Users”. In Proceedings of the 32th Web Conference.
- **[ISSTA 2022W]** **Ziqi Zhang**, Lucien K. L. Ng, Yifeng Cai, Yao Guo, Bingyan Liu, Ding Li, and Xiangqun Chen. “TEESlice: Slicing DNN Models for Secure and Efficient Deployment inside TEEs”. AISTA Workshop @ ISSTA 2022.
- **[Ubicomp 2022]** Bingyan Liu, Yifeng Cai, **Ziqi Zhang**, Yuanchun Li, Leye Wang, Ding Li, Yao Guo, Xiangqun Chen. “DistFL: Distribution-aware Federated Learning for Mobile Scenarios”. In ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.
- **[ISSTA 2021]** Yuanchun Li*, **Ziqi Zhang***, Bingyan Liu, Ziyue Yang, Yunxin Liu. “ModelDiff: Testing-based DNN Similarity Comparison for Model Reuse Detection”. In Proceedings of the 30th ACM SIGSOFT International Symposium on Software Testing and Analysis.

Teaching Experience

Teaching Assistant, Operating System (Honor Track, JOS), Peking University	Fall 2021
Teaching Assistant, Operating System (Honor Track, JOS), Peking University	Fall 2020
Teaching Assistant, Operating System (Honor Track, JOS), Peking University	Spring 2020
Teaching Assistant, Operating System (Honor Track, JOS), Peking University	Fall 2019
Teaching Assistant, Algorithm Design and Analysis, Peking University	Spring 2019

Service

Program Committee Member, The ACM International Conference on the Foundations of Software Engineering (FSE)	2026
Program Committee Member, The 40th IEEE/ACM International Conference on Automated Software Engineering (ASE)	2024, 2025
Artifact Evaluation Committee Member, The ACM Conference on Computer and Communications Security (CCS)	2025
Program Committee Member, International Workshop on Large Language Models for Code (LLM4Code)	2024, 2025, 2026
Student/Postdoc AMA Panelist, Midwest Security Workshop	2024, 2025

Awards

Outstanding Doctoral Dissertation Award	Jun 2023
Outstanding Graduate Award of Peking University	Jun 2023
Merit Student, Peking University	Sep 2022
Jiukun Scholarship, Peking University	Sep 2022
Stars of Tomorrow Intership Program, Microsoft Research Asia	Sep 2020
Intel Scholarship, Intel	Dec 2019

Invited Talks

Midwest Security Workshop, Purdue University	Nov 2024
KFSCIS Seminar Series, Florida International University	Oct 2024
UIUC CS591 Security Seminar, Urbana	Sep 2024
S&P 2024, San Francisco	May 2024
Secret Flow, Ant Group	Dec 2023
Security Group, TouTiao	Dec 2023
NetSys weekly seminar, Imperial College London	Nov 2023
Secret Flow, Ant Group	Aug 2023
The 45th International Conference on Software Engineering, Australia Melbourne	May 2022
The 31st International Symposium on Software Testing and Analysis, Virtual Event	Jun 2022
The 44th International Conference on Software Engineering, Virtual Event	May 2022
The 28th ESEC/FSE Conference, Virtual Event	Nov 2020

Internship

Ant Group, Beijing, China 2023.02 – 2024.02

Part-Time Research Intern
Mentor: Ruoyu Li
Project: Study security and privcy issues in AliPay mini-apps

Microsoft Research Aisa, Beijing, China 2020.02 – 2020.08

Full-Time Research Intern
Mentor: Yuanchun Li, Yunxin Liu
Project: Model slicing technique to reduce defect inheritance in transfer learning