Ziqi Zhang

Gender: Male · Age: 29 · · Email: ziqi_zhang@pku.edu.cn

Research Interest

Research topic: Trusted AI, Security of DNN models, Software engineering for AI models
Rsearch goal: Making DNN models more secure, reliable, and robust.

- TEE-based Model Protection: TEE-Shielded DNN Partition (ISSTA'22W, S&P'24, ICML'24)
- Software Engineering and AI: model slicing (ESEC/FSE'20, ICSE'22), model testing (ISSTA'21)
- Privacy: federated learning (ICSE'23, Ubicomp'22, WWW'23, Security'24)

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

- **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 Proceedings of IEEE S&P 2024. (**CCF-A**)
- **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 International Conference on Software Engineering (ICSE 2023). (**CCF-A**, 209/796=26.2%)
- **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 International Conference on Software Engineering (ICSE 2022). (**CCF-A**, 197/751≈26.2%)
- **Ziqi Zhang**, Yuanchun Li, Yao Guo, Xiangqun Chen, Yunxin Liu. "Dynamic Slicing for Deep Neural Networks." In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2020). (**CCF-A**, 101/360≈28.0%)

Other Publications

- 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" USENIX Security (**CCF-A**, Accepted).
- 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 International Conference on Machine Learning (**CCF-A**, 2609/9653=27.03%).
- 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 IEEE International Symposium on Software Reliability Engineering (ISSRE), 2023. (**CCF-B**, Accepted)

- 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 ACM Conference on Computer and Communications Security (CCS), 2023. (**CCF-A**, 158/795=19.87%).
- 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 ACM Conference on Computer and Communications Security (CCS), 2023. (**CCF-A**, 158/795=19.87%).
- 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 (WWW 2023). (**CCF-A**, 365/1900=19.2%)
- **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, Accepted.
- 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 (Ubicomp 2022). (**CCF-A**)
- Yuanchun Li, **Ziqi Zhang**, Bingyan Liu, Ziyue Yang, Yunxin Liu. "ModelDiff: Testing-based DNN Similarity Comparison for Model Reuse Detection". The ACM SIGSOFT International Symposium on Software Testing and Analysis. (ISSTA 2021). (**CCF-A**, 51/233=21.9%)

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

Internship

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

Selected Honors

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

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