Qingzhao Zhang

(+1) 734-881-5608 | qzzhang@umich.edu | Github: zqzqz |
Website: https://zqzqz.github.io/ | Google Scholar | LinkedIn

EDUCATION

University of Michigan, Department of Computer Science and Engineering Sep 2019-Present
Ph.D. student, Overall GPA: 3.98/4.0
School of Cyber Security, Shanghai Jiao Tong University (SJTU) Oct 2015-June 2019
B.E. in Cyber Security, Overall GPA: 89.63/100, Major GPA: 90.62/100, Rank: 5/96

INTERESTS

System security (e.g., cyber-physical systems, autonomous driving), software security (e.g., program analysis, formal verification), AI security (e.g., adversarial attacks, robustness).

WORK EXPERIENCES

Robustnet Lab | Research Assistant | University of Michigan, Ann Arbor Sep 2019-Present
Advisor: Z. Morley Mao, Professor, University of Michigan

- Research on software/system for cyber-physical system safety — *AVChecker*, the first traffic rule compliance checker on autonomous driving software; *SmtConf*, safety vetting of industrial control system configuration.
- Research on adversarial machine learning on cyber-physical systems — Adversarial attack and mitigation on trajectory prediction on autonomous driving; Analyzed data fabrication vulnerability on collaborative perception.
- Research on robustness of vehicular network — *RAO*, collaborative perception with asynchronous sensors.
- Research on robust perception algorithms of autonomous driving, and large language model security/efficiency.

Google | Software Engineer Intern | Mountain View, CA May 2023-July 2023

- Skills: model checking, theorem proving, operating systems, Rust, Python
- Designed and implemented formal verification solutions to enhance the security properties of an embedded system kernel (based on open-sourced Tock OS), involving modular model checking and theorem proving.

Google | Software Engineer Intern | Sunnyvale, CA May 2022-July 2022

- Skills: static analysis, Android, Kotlin
- Designed and implemented static analysis checks based on Android Lint for Google's Android tests, which was deployed to assist Google developers to write high-quality unit tests.

YITU Technology | Software Engineer Intern | Shanghai May 2019-July 2019

- Skills: Web, SpringBoot, Java, Python
- Implemented Web APIs for face recognition applications in the company's production.

Automated Software Engineering group | Visiting Student | UIUC Jul 2018-Oct 2018
Advisor: Tao Xie, professor and Willett Faculty Scholar, UIUC | Bo Li, assistant professor, UIUC

- Designed blockchain-based decentralized advertising systems using public smart contracts.
- Research on vulnerability detection and automatic repair of real-world smart contracts (Ethereum).

Lab of Cryptology and Computer Security| Research Assistant | SJTU May 2017-May 2019
Advisor: Haining Lu & Ning Ding, researcher at Lab of Cryptology and Computer Security, SJTU

- Research on vulnerability detection of smart contracts — designed an efficient smart contract fuzzer *EthPloit*.
- Collaborated in designing protocols of privacy-preserving permissioned blockchain with ring signatures or zero-knowledge proof.

PUBLICATIONS

(* — co-first authors)

Conference publications

- CALICO: Self-Supervised Camera-LiDAR Contrastive Pre-training for BEV Perception
  Jiachen Sun, Haizhong Zheng, **Qingzhao Zhang**, Atul Prakash, Z. Morley Mao, Chaowei Xiao
  The 12th International Conference on Learning Representations (ICLR 2024)

- On Data Fabrication in Collaborative Vehicular Perception: Attacks and Countermeasures
  Qingzhao Zhang, Shuowei Jin, Ruiyang Zhu, Jiachen Sun, Xumiao Zhang, Q. Alfred Chen, Z. Morley Mao
  The 33th USENIX Security Symposium (USENIX Security 2024).

- Robust Real-time Multi-vehicle Collaboration on Asynchronous Sensors
  Qingzhao Zhang*, Xumiao Zhang*, Ruiyang Zhu*, Fan Bai, Mohammad Naserian, Z. Morley Mao
  The 29th International Conference on Mobile Computing and Networking (MobiCom 2023).

- On Adversarial Robustness of Trajectory Prediction for Autonomous Vehicles
  Qingzhao Zhang, Shengtuo Hu, Jiachen Sun, Qi Alfred Chen, Z. Morley Mao.
  Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2022)

- Automated Runtime Mitigation for Timing-based Safety Hazards in Industrial Controllers
  Qingzhao Zhang, Xiao Zhu, Mu Zhang, Z. Morley Mao.
  The 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)

- GateKeeper: A Gateway-based Broadcast Authentication Protocol for the In-vehicle Ethernet
  Shengtuo Hu, **Qingzhao Zhang**, André Weimerskirch, Z Morley Mao
  Proceedings of the ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2022)

- AVMaestro: A Centralized Policy Enforcement Framework for Safe Autonomous-driving Environments
  Ze Zhang, Sanjay Sri Vallabh Singapuram, **Qingzhao Zhang**, David Ke Hong, Brandon Nguyen, Z Morley Mao, Scott Mahlke, Qi Alfred Chen
  2022 IEEE Intelligent Vehicles Symposium (IV 2022)

- A Systematic Framework for Checking Driving Rule Compliance in Autonomous Vehicle Software
  Qingzhao Zhang, David Ke Hong, Ze Zhang, Qi Alfred Chen, Scott Mahlke, Z. Morley Mao.
  Proceedings of the ACM on Measurement and Analysis of Computing Systems (SIGMETRICS 2021)

- EthPloit: From Fuzzing to Efficient Exploit Generation against Smart Contracts
  Qingzhao Zhang*, Yizhuo Wang*, Juanru Li, Siqi Ma.
  IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER 2020)

- Ringct 3.0 for blockchain confidential transaction: Shorter size and stronger security
  Tsz Hon Yuen, Shi-feng Sun, Joseph K Liu, Man Ho Au, Muhammed F Esgin, **Qingzhao Zhang**, Dawu Gu
  Financial Cryptography and Data Security: 24th International Conference (FC 2020)

Journal publications

- PBT: A New Privacy-Preserving Payment Protocol for Blockchain Transactions
  Yanxue Jia, Shi-Feng Sun, Yuncong Zhang, **Qingzhao Zhang**, Ning Ding, Zhiqiang Liu, Joseph K Liu, Dawu Gu, IEEE Transactions on Dependable and Secure Computing

Workshop publications

- Stealthy Data Fabrication in Collaborative Vehicular Perception
  Qingzhao Zhang, Z. Morley Mao
  The 6th Workshop on CPS and IoT Security (CPSIoTSec 2024)

- ModelNet40-C: A Robustness Benchmark for 3D Point Cloud Recognition Under Corruption
  Jiachen Sun, **Qingzhao Zhang**, Bhavya Kailkhura, Zhiding Yu, Chaowei Xiao, Z Morley Mao

ICLR 2022 Workshop on Socially Responsible Machine Learning (SRML 2022)

- Automatic Feature Isolation in Network Protocol Software Implementations
  Ze Zhang, **Qingzhao Zhang**, Brandon Nguyen, Sanjay Sri Vallabh Singapuram, Z Morley Mao, Scott Mahlke
  ACM Workshop on Forming an Ecosystem Around Software Transformation (FEAST 2020)

Preprints

- Safeguard is a Double-edged Sword: Denial-of-service Attack on Large Language Models
  Qingzhao Zhang, Ziyang Xiong, Z. Morley Mao

- Compute Or Load KV Cache? Why Not Both?
  Shuowei Jin, Xueshen Liu, **Qingzhao Zhang**, Z. Morley Mao

- Cocoon: Robust Multi-Modal Perception with Uncertainty-Aware Sensor Fusion
  Minkyoung Cho, Yulong Cao, Jiachen Sun, **Qingzhao Zhang**, Marco Pavone, Jeong Joon Park, Heng Yang, Z. Mao

- Adaptive Skeleton Graph Decoding
  Shuowei Jin, Yongji Wu, Haizhong Zheng, **Qingzhao Zhang**, Matthew Lentz, Z Morley Mao, Atul Prakash, Feng Qian, Danyang Zhuo

- Exploring the Limits of ChatGPT in Software Security Applications
  Fangzhou Wu, **Qingzhao Zhang**, Ati Priya Bajaj, Tiffany Bao, Ning Zhang, Ruoyu Wang, Chaowei Xiao

- Partial-Information, Longitudinal Cyber Attacks on LiDAR in Autonomous Vehicles
  R Spencer Hallyburton, **Qingzhao Zhang**, Z. Morley Mao, Miroslav Pajic

- Benchmarking Robustness of 3d Point Cloud Recognition Against Common Corruptions
  Jiachen Sun, **Qingzhao Zhang**, Bhavya Kailkhura, Zhiding Yu, Chaowei Xiao, Z. Morley Mao

In submission

- StreetCred: A Privacy-Preserving Reputation System for Connected Autonomous Vehicles
  Anrin Chakraborti*, **Qingzhao Zhang***, Jingjia Peng, Z. Morley Mao, Michael K. Reiter

- RAO++: Realistic Real-time Multi-vehicle Collaboration on Asynchronous Sensors
  Ruiyang Zhu, **Qingzhao Zhang**, Xumiao Zhang, Fan Bai, Mohammad Naserian, Z. Morley Mao

TEACHING & MENTORSHIP

Supervisor of Multidisciplinary Design Program (Undergraduate Research), University of Michigan 2022

- Four undergraduate students, two-semester project, cybersecurity research.

Research mentorship of undergraduate/graduate students 2020-2024

- Mentees: Charles Ziegenbein Jr., Kevin Zhang, Andrew Wei, Xingyu Wang, Jingjia Peng, Ziyang Xiong.
- Research on program analysis, autonomous driving, adversarial machine learning.

SERVICES

Reviewer, ICLR	2025
Reviewer, ICRA	2025
Pre-review program committee, NSDI 2025	2025
Reviewer, ACM Multimedia	2024
Reviewer, IEEE Internet of Things Journal	2024
Reviewer, IEEE Intelligent Transportation Systems Magazine	2023-2024
Reviewer, IEEE Transactions on Intelligent Vehicles (IV)	2023-2024
Reviewer, 5G/6G Precise Positioning on C-ITS and CAV	2023
Reviewer, Workshop on Re-design Industrial Control Systems with Security (RICSS)	2023, 2024

Reviewer, Transactions on Dependable and Secure Computing (TDSC)	2022
Artifact Evaluation Reviewer, Usenix Security	2022

TALKS

Stealthy Data Fabrication in Collaborative Vehicular Perception

- 10/18/2024: Presentation at 6th CPSIoTSec Workshop, co-located with CCS 2024.

On data fabrication in collaborative vehicular perception: attacks and countermeasures

- 5/3/2023: Poster at Athena institute (NSF AI Institute) annual showcase (**best poster award**)
- 8/16/2024: Presentation at USENIX Security 2024

Automated runtime mitigation for timing-based safety hazards in industrial controllers

- 10/27/2022: Virtual presentation at RAID 2022

On adversarial robustness of trajectory prediction for autonomous vehicles

- 8/18/2022: Poster at Athena institute (NSF AI Institute) annual showcase
- 6/23/2022: Poster at CVPR 2022

Robustness of applications for autonomous vehicles

- 11/19/2021: Presentation at Workshop on Future Automotive Research Datasets

A systematic framework for checking driving rule compliance in autonomous vehicle software

- 6/16/2021: Virtual presentation at SIGMETRICS 2021

HONORS & AWARDS

Usenix Security, SIGMETRICS, CCS Student Travel Grant	2020-2024
Student Fellowship	2019
Academic Excellence Scholarship of SJTU, B Class (top 5%)	2016, 2017, 2018