Alfred Chen

Assistant Professor
Department of Computer Science
University of California, Irvine
Email: alfchen@uci.edu

Office: ICS1 420, Inner Ring Rd, Irvine, CA 92617
Tel: 949-824-7865
Homepage: https://www.ics.uci.edu/~alfchen

EDUCATION

- **Ph.D. in Computer Science and Engineering**, University of Michigan, Ann Arbor 2018
  – *Dissertation*: "Proactive Vulnerability Discovery and Assessment in Smart, Connected Systems Through Systematic Problem Analysis"
  – *Committee*: Prof. Z. Morley Mao (chair), Prof. Atul Prakash, Prof. Michael Reiter, Prof. Henry Liu, and Prof. Zhiyun Qian
  – **ProQuest Distinguished Dissertation Award** (top 10 in University of Michigan, across all graduate schools ranging from science and engineering to archaeology and history)
  – Nominated for *ACM Doctoral dissertation Award*
- **B.S. in Department of Computer Science and Technology**, Nanjing University, Nanjing, China 2012
  – *Top 100 Excellent Undergraduate Students of the Year*, China Computer Federation (2012, top 100 in China)

WORK EXPERIENCE

- *Jul. 2018 - Now* **Assistant Professor, Department of Computer Science**, University of California, Irvine
  – Lead the AS^{2}Guard (Autonomous & Smart Systems Guard) research group focusing on **security/privacy** issues in emerging AI/systems/network technologies, especially the latest ones with high societal impacts such as those powering the emerging AI-enabled autonomous cars/drones/robots, intelligent transportation, smart home, etc.
  – **Intellectural metrit**: ***First*** to perform security analysis and/or defense designs on various mission- and safety-critical industry-grade AD (Autonomous Driving) AI components such as perception (ACM CCS'19, Usenix Security'21, IEEE S&P'21, ICCV'23, NDSS'24), object tracking (ICLR'20), localization (Usenix Security'21, IROS'23), lane detection (Usenix Security'21, IV'21, CVPR'22), multi-sensor fusion (Usenix Security'21, IEEE S&P'21, IROS'23), prediction (CVPR'22, IROS'23, ICCV'23), and planning (NDSS'22); ***First*** to develop formal verification methods for cooperative AD such as platooning (Usenix Security'21) and traffic rule conformation (ACM Sigmetrics'21); ***First*** to characterize AD software bugs (ICSE'20); and ***First*** to perform security analysis of USDOT's intelligent traffic signal control (NDSS'18, TRB/TRR'18, T-ITS'22), and design defense solutions at both infrastructure and vehicle sides (TRB'19, IV'23).
  – **Broader impacts**: Triggered ***>30 AD companies*** (e.g., Tesla, GM, Daimler, Baidu, TuSimple, Aptiv, Hyundai, Volkswagen, Bosch, Lyft, Nuro, Toyota, Kia, Volvo) and ***IEEE 1609 Workgroup*** (for CV/V2X protocol standardization) to start investigating newly-discovered security vulnerabilities, some confirmed to work on fixes; invited to speak about these research at GM, Toyota, IBM, NVIDIA, Qualcomm, NHTSA (National Highway Traffic Safety Administration) VRTC, Auto-ISAC Summit'21,'24, ACM AsiaCCS CPSS'21 (***keynote***), AUTOSAR Open Conference'23 (***keynote***), etc.
  – **Community impacts**: ***Co-founded*** the ISOC Symposium on Vehicle Security & Privacy (VehicleSec) in 2023, which is built upon 4 years of community growth developed by the AutoSec (Automotive & Autonomous Vehicle Security) Workshop (also ***co-found*** by me, co-located with NDSS since 2021, one of the "big 4" top-tier security conferences); ***Co-created*** DEF CON's first AutoDriving-themed hacking event in 2021 (DEF CON is one of world's largest & most notable hacker conventions), serve as co-organizor anually from 2021 till now (2023); *Co-chair* the IEEE SafeThings Workshop with IEEE S&P'21; Served as PC for top-tier venues such as IEEE S&P'24, Usenix Security'21-24, NDSS'22-23, ACM CCS'21,'23, CVPR'22-23, ECCV'22, NeurIPS'23, ICRA'23, IROS'23, INFOCOM'23, etc.
  – **Education/mentoring**: Created a ***new*** graduate-level security course (CS205, ***core course*** since 2022); mentor 7 Ph.D., 9 M.S., 32 B.S. (**over 10 URMs**); faculty advisor for Cyber@UCI (undergraduate cybersecurity club).
  – **Awards**: **NSF *CAREER Award***; NDSS'20 Best Technical Poster Award; NDSS'19 Distinguished Poster Presentation Award; Talk awards at HotSec'19 (co-located w/ Usenix Security); UC Irvine Chancellor's Award for Excellence in Undergraduate Research Mentorship (***1 faculty per school***); (as faculty advisor) ***1st place (champion)*** on Baidu Security Autonomous Driving Security CTF competition; and (as faculty advisor) ***1st place (Gold Medal)*** on CCDC (Collegiate Cyber Defense Competition) Western Regional, advanced to National CCDC for the ***first time***, and ended up ***5th place out of 168+ university/college teams*** nation-wide at National CCDC.

- *Sept. 2012 - Aug. 2018* **Research Assistant, RobustNet Research Group**, University of Michigan, Ann Arbor
  Advisor: Professor Z. Morley Mao (University of Michigan)
  – **Awards**: *ProQuest Distinguished Dissertation Award*, *Rackham Predoctoral Fellowship*, nominated for Microsoft Research PhD Fellowship and ACM Doctoral dissertation Award

- *May 2015 - Oct. 2015* **Research Intern**, Verisign Labs, Reston
  Mentor: Eric Osterweil (Principal Scientist, Verisign Labs), and Matthew Thomas (Data Architect, Verisign Labs)

AWARDS AND HONORS

- **NSF CAREER Award** on securing emerging autonomous and connected CPSs (e.g., autonomous cars, drones, and robots), NSF SaTC (Secure & Trustworthy Cyberspace) Program (2022)
- Invited by the IEEE Intelligent Transportation Systems Society to serve on the IEEE Emerging Transportation Technology Testing (ET3) Technical Committee. (2023, *the only committee member from CS*)
- **2nd place (Silver Medal)**, CCDC (Collegiate Cyber Defense Competition) Western Regional competition (2022, as faculty advisor, *top 1/22* in western region)
- Invited by NIST to serve on the AI panel & focused group on standards and performance metrics development for on-road autonomous vehicles (2022, *the only invitee on related AI security research*)
- **Chancellor's Award for Excellence in Undergraduate Research Mentorship**, UC Irvine (2021, *1 faculty per school*)
- **5th place nation-wide**, National CCDC (Collegiate Cyber Defense Competition) competition (2021, as faculty advisor, *top 5 out of 168+ universities/colleges nation-wide*)
- **1st place (Gold Medal)**, CCDC (Collegiate Cyber Defense Competition) Western Regional competition (2021, as faculty advisor, *top 1/18* in western region, beating strong rivals such as Stanford, *advanced to National CCDC for the first time*)
- Invited to speak at 5th Annual Auto-ISAC Cybersecurity Summit, GM Marriott at the Renaissance Center, Detroit (2021, *the only invited speaker on related academic research*)
- **1st place (champion)**, Baidu Autonomous Driving Security CTF competition (2020, as faculty advisor, *top 1/24*)
- **Best Technical Poster Award** for "Security of Deep Learning based Lane Keeping Assistance System under Physical-World Adversarial Attack" at ISOC NDSS 2020 (2020, *top 1/30*)
- Most Amusing Award and Most Engaging Award for talk "Ghost Cars & Fake Obstacles: First Look at Control Software Stack Security in Emerging Smart Transportation" at 2019 USENIX Summit on Hot Topics in Security (HotSec'19) (2019, *both top 1/17*)
- **Distinguished Poster Presentation Award** for "Security Analysis of Multi-Sensor Fusion based Localization in Autonomous Vehicles" at ISOC NDSS 2019 (2019, *top 2/36*)
- **ProQuest Distinguished Dissertation Award**, University of Michigan (2019, *top 10 in University of Michigan*, across *all* graduate schools ranging from science and engineering to archaeology and history)
- Rackham Predoctoral Fellowship, Rackham School, University of Michigan (2017, *1-2 each dept.* to support students working on dissertation that are unusually creative, ambitious and risk-taking)
- **Top 100 Excellent Undergraduate Students of the Year**, China Computer Federation (2012, *top 100 in China*)

PUBLICATIONS

Summary

Total Citations: **3910**, H-Index: **29**, i10-Index: **56** (Google Scholar, as of Janurary 2024)

21 in commonly-recognized top-tier security conferences (IEEE Security & Privacy, USENIX Security, ACM CCS, NDSS)

9 in commonly-recognized top-tier networking/mobile/systems conferences (ACM IMC, ACM MobiSys, ACM MobiCom, ACM Sigmetrics, EuroSys)

8 in commonly-recognized top-tier transportation/automobile conferences/journals (T-ITS, TRB/TRR, IEEE IV)

6 in commonly-recognized top-tier artificial intelligence conferences (CVPR, ICCV, ICLR, AAAI)

3 in commonly-recognized top-tier software engineering conferences/journals (ICSE, TSE)

2 in commonly-recognized top-tier robotics conferences (IROS)

Conference/Workshop Publications

(top-tier conferences are highlighted in **bold**; students mentored by me are underlined)

C75. **[NDSS'24]** Takami Sato, Yuki Hayakawa, Ryo Suzuki, Yohsuke Shiiki, Kentaro Yoshioka, and **Qi Alfred Chen**, LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies, ISOC Network and Distributed System Security Symposium (NDSS) 2024. *(acceptance rate (summer cycle) 19.9% = 42/211).*

C74. **[NDSS'24]** Takami Sato, Sri Hrushikesh Varma Bhupathiraju, Michael Clifford, Takeshi Sugawara, **Qi Alfred Chen**, and Sara Rampazzi, Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception, ISOC

Network and Distributed System Security Symposium (NDSS) 2024. *(acceptance rate TBD)*.

C73. **[Usenix Security'24]** Qingzhao Zhang, Shuowei Jin, Ruiyang Zhu, Jiachen Sun, Xumiao Zhang, **Qi Alfred Chen**, and Z. Morley Mao, On Data Fabrication in Collaborative Vehicular Perception: Attacks and Countermeasures, USENIX Security Symposium 2024. *(acceptance rate TBD)*.

C72. **[Usenix Security'24]** Shuo Wang, Hongsheng Hu, Hannan Zhong, Jiamin Chang, Benjamin Zi Hao Zhao, **Qi Alfred Chen**, and Minhui Xue, DNN-GP: Diagnosing and Mitigating Model's Faults Using Latent Concepts, USENIX Security Symposium 2024. *(acceptance rate TBD)*.

C71. **[AAAI'24]** Chen Ma, Ningfei Wang, **Qi Alfred Chen**, and Chao Shen, SlowTrack: Increasing the Latency of Camera-based Perception in Autonomous Driving Using Adversarial Examples, Annual AAAI Conference on Artificial Intelligence (AAAI) 2024. *(acceptance rate 23.7% = 2342/9862)*.

C70. [VehicleSec'24] Wentao Chen, Sam Der, Yunpeng Luo, Fayzah Alshammari, and **Qi Alfred Chen**, Understanding the Internet-Wide Vulnerability Landscape for ROS-based Robotic Vehicles, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2024.

C69. [VehicleSec'24] Sri Hrushikesh Varma Bhupathiraju, Takami Sato, Michael Clifford, Takeshi Sugawara, **Qi Alfred Chen**, and Sara Rampazzi, On the Vulnerability of Traffic Light Recognition Systems to Laser Illumination Attacks, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2024.

C68. [VehicleSec'24] Takami Sato, Ningfei Wang, Yueqiang Cheng, and **Qi Alfred Chen**, A Cross-Verification Approach with Publicly Available Map for Detecting Off-Road Attacks against Lane Detection Systems, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2024.

C67. **[ICCV'23]** Ningfei Wang, Yunpeng Luo, Takami Sato, Kaidi Xu, and **Qi Alfred Chen**, Does Physical Adversarial Example Really Matter to Autonomous Driving? Towards System-Level Effect of Adversarial Object Evasion Attack, International Conference on Computer Vision (ICCV) 2023. *(acceptance rate 26.8% = 2160/8068)*.

C66. **[ICCV'23]** Ruochen Jiao, Xiangguo Liu, Takami Sato, **Qi Alfred Chen**, and Qi Zhu, Semi-supervised Semantics-guided Adversarial Training for Robust Trajectory Prediction, International Conference on Computer Vision (ICCV) 2023. *(acceptance rate 26.8% = 2160/8068)*.

C65. **[ICSE'23]** Yuqi Huai, Yuantianyi Chen, Sumaya Almanee, Tuan Ngo, Xiang Liao, Ziwen Wan, **Qi Alfred Chen**, and Joshua Garcia, Doppelganger Test Generation for Revealing Bugs in Autonomous Driving Software, International Conference on Software Engineering (ICSE) 2023. *(acceptance rate 26.3% = 209/796)*.

C64. **[IROS'23]** Junjie Shen, Ziwen Wan, Yunpeng Luo, and **Qi Alfred Chen**, Lateral-Direction Localization Attack in High-Level Autonomous Driving: Domain-Specific Defense Opportunity via Lane Detection, IEEE/RSJ International Conference on Intelligent Robots (IROS) 2023.

C63. **[IROS'23]** Ruochen Jiao, Juyang Bai, Xiangguo Liu, Takami Sato, Xiaowei Yuan, **Qi Alfred Chen**, and Qi Zhu, Learning Representation for Anomaly Detection of Vehicle Trajectories, IEEE/RSJ International Conference on Intelligent Robots (IROS) 2023.

C62. **[IV'23]** Junjie Shen, Ziwen Wan, Yunpeng Luo, Yiheng Feng, Z. Morley Mao, and **Qi Alfred Chen**, Detecting Data Spoofing in Connected Vehicle Based Intelligent Traffic Signal Control Using Infrastructure-Side Sensors and Traffic Invariants, IEEE Intelligent Vehicles Symposium (IV) 2023.

C61. [VehicleSec'23] Takami Sato*, Sri Hrushikesh Varma Bhupathiraju* (co-first authors), Michael Clifford, Takeshi Sugawara, **Qi Alfred Chen**, and Sara Rampazzi, WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2023.

C60. [VehicleSec'23] Jun Ying, Yiheng Feng, **Qi Alfred Chen**, and Z. Morley Mao, GPS Spoofing Attack Detection on Intersection Movement Assist using One-Class Classification, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2023.

C59. [VehicleSec'23] Takami Sato, Yuki Hayakawa, Ryo Suzuki, Yohsuke Shiiki, Kentaro Yoshioka, and **Qi Alfred Chen**, WIP: Practical Removal Attacks on LiDAR-based Object Detection in Autonomous Driving, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2023.

C58. [VehicleSec'23] Chen Ma, Ningfei Wang, **Qi Alfred Chen**, and Chao Shen, WIP: Towards the Practicality of the Adversarial Attack on Object Tracking in Autonomous Driving, ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2023.

C57. **[DAC'23 Invited]** Xiangguo Liu, Yunpeng Luo, Anthony Goeckner, Trishna Chakraborty, Ruochen Jiao, Ningfei Wang, Yixuan Wang, Takami Sato, **Qi Alfred Chen**, and Qi Zhu, Invited: Waving the Double-Edged Sword: Building Resilient CAVs with Edge and Cloud Computing, ACM/IEEE Design Automation Conference (DAC) 2023.

C56. **[NDSS'22]** Ziwen Wan, Junjie Shen, Jalen Chuang, Xin Xia, Josh Garcia, Jiaqi Ma, and **Qi Alfred Chen**, Too Afraid to Drive: Systematic Discovery of Semantic DoS Vulnerability in Autonomous Driving Planning under Physical-World Attacks, ISOC Network and Distributed System Security Symposium (NDSS) 2022. *(acceptance rate 16.2% = 83/513)*.

C55. **[CVPR'22]** Takami Sato, and **Qi Alfred Chen**, Towards Driving-Oriented Metric for Lane Detection Models, IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2022. *(acceptance rate 25.3% = 2067/8161)*.

C54. **[CVPR'22]** Qingzhao Zhang, Shengtuo Hu, Jiachen Sun, **Qi Alfred Chen**, and Z. Morley Mao, On Adversarial Robustness of Trajectory Prediction for Autonomous Vehicles, IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2022. *(acceptance rate 25.3% = 2067/8161)*.

C53. **[IV'22]** Ze Zhang, Sanjay Sri Vallabh Singapuram, Qingzhao Zhang, David Ke Hong, Brandon Nguyen, Z Morley Mao, Scott Mahlke, and **Qi Alfred Chen**, AVMaestro: A Centralized Policy Enforcement Framework for Safe Autonomous-driving Environments, IEEE Intelligent Vehicles Symposium (IV) 2022.

C52. [ACSAC'22] Qifan Zhang, Junjie Shen, Mingtian Tan, Zhe Zhou, Zhou Li, **Qi Alfred Chen**, and Haipeng Zhang, Play the Imitation Game: Model Extraction Attack against Autonomous Driving Localization, Annual Computer Security Applications Conference (ACSAC) 2022.

C51. [AutoSec'22] Yunpeng Luo, Ningfei Wang, Bo Yu, Shaoshan Liu, and **Qi Alfred Chen**, Infrastructure-Aided Defense for Autonomous Driving Systems: Opportunities and Challenges, ISOC NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022.

C50. [AutoSec'22] Zhisheng Hu, Junjie Shen, Shengjian Guo, Xinyang Zhang, Zhenyu Zhong, **Qi Alfred Chen**, and Kang Li, PASS: A System-Driven Evaluation Platform for Autonomous Driving Safety and Security, ISOC NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022.

C49. **[S&P'21]** Yulong Cao*, Ningfei Wang*, Chaowei Xiao*, Dawei Yang* (co-first authors), Jin Fang, Ruigang Yang, **Qi Alfred Chen**, Mingyan Liu, and Bo Li, Invisible in both Camera and LiDAR: Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks, IEEE Symposium on Security and Privacy (S&P) 2021. *(acceptance rate 12.0% = 117/972)*

C48. **[USENIX Security'21]** Takami Sato*, Junjie Shen* (co-first authors), Ningfei Wang, Yunhan Jia, Xue Lin, and **Qi Alfred Chen**, Dirty Road Can Attack: Security of Deep Learning based Automated Lane Centering under Physical-World Adversarial Attack, USENIX Security Symposium 2021. *(acceptance rate 18.7% = 246/1316)* **NDSS'20 Best Technical Poster Award**

C47. **[USENIX Security'21]** Shengtuo Hu, **Qi Alfred Chen**, Jiachen Sun, Yiheng Feng, Z. Morley Mao, and Henry X. Liu, Automated Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Protocols, USENIX Security Symposium 2021. *(acceptance rate 18.7% = 246/1316)*

C46. **[IV'21]** Ruochen Jiao, Hengyi Liang, Takami Sato, Junjie Shen, **Qi Alfred Chen**, and Qi Zhu, End-to-end Uncertainty-based Mitigation of Adversarial Attacks to Automated Lane Centering, IEEE Intelligent Vehicles Symposium (IV) 2021.

C45. **[Sigmetrics'21]** Qingzhao Zhang, David Ke Hong, Ze Zhang, **Qi Alfred Chen**, Scott Mahlke, and Z. Morley Mao, A Systematic Framework to Identify Violations of Scenario-dependent Driving Rules in Autonomous Vehicle Software, ACM International Conference on Measurement and Modeling of Computer Systems (Sigmetrics) 2021. *(acceptance rate (winter) 12.1%=15/124)*

C44. **[Mobicom'21]** Di Gao, Hao Lin, Zhenhua Li, Feng Qian, **Qi Alfred Chen**, Zhiyun Qian, Wei Liu, Liangyi Gong, and Yunhao Liu, A Nationwide Census on WiFi Security Threats: Prevalence, Riskiness, and the Economics, ACM Annual International Conference on Mobile Computing and Networking (Mobicom) 2021. *(acceptance rate 15.1%=19/126)*

C43. [BMVC'21] Siyue Wang, Pu Zhao, Xiao Wang, Sang Chin, Thomas Wahl, Yunsi Fei, **Qi Alfred Chen**, and Xue Lin, Intrinsic Examples: Robust Fingerprinting of Deep Neural Networks, British Machine Vision Conference (BMVC) 2021. *(acceptance rate 36.2%=437/1206)*

C42. [BMVC'21] Jiachen Sun, Karl Koenig, Yulong Cao, **Qi Alfred Chen**, and Z. Morley Mao, On Adversarial Robustness of 3D Point Cloud Classification under Adaptive Attacks, British Machine Vision Conference (BMVC) 2021. *(acceptance rate 36.2%=437/1206)*

C41. [AutoSec'21] Kanglan Tang, Junjie Shen, and **Qi Alfred Chen**, Fooling Perception via Location: A Case of Region-of-Interest Attacks on Traffic Light Detection in Autonomous Driving, ISOC NDSS Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021.

C40. [SRDS'21] Tong Chen, Yingxiao Xiang, Yike Li, Yunzhe Tian, Endong Tong, Wenjia Niu, Jiqiang Liu, Gang Li, and **Qi Alfred Chen**, Protecting Reward Function of Reinforcement Learning via Minimal and Non-catastrophic Adversarial Trajectory, 40th International Symposium on Reliable Distributed Systems (SRDS), 2021. *(acceptance rate 25.5%=27/106)*

C39. [ICIP'21] Won Park, Nan Li, **Qi Alfred Chen**, and Z. Morley Mao, Sensor Adversarial Traits: Analyzing Robustness of 3D Object Detection Sensor Fusion Models, IEEE International Conference on Image Processing (ICIP) 2021. *(acceptance rate 45.9%=791/1722)*

C38. **[USENIX Security'20]** Junjie Shen, Jun Yeon Won, Zeyuan Chen, and **Qi Alfred Chen**, Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing, USENIX Security Symposium 2020. *(acceptance rate 16.1%=157/977)* **NDSS'19 Distinguished Poster Presentation Award**

C37. **[USENIX Security'20]** Jiachen Sun, Yulong Cao, **Qi Alfred Chen**, and Z. Morley Mao, Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures, USENIX Security Symposium 2020. *(acceptance rate 16.1%=157/977)*

C36. **[USENIX Security'20]** Haohuang Wen, **Qi Alfred Chen**, and Zhiqiang Lin, Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT, USENIX Security Symposium 2020. *(acceptance rate 16.1%=157/977)*

C35. **[NDSS'20]** Haohuang Wen, Qingchuan Zhao, **Qi Alfred Chen**, and Zhiqiang Lin, Automated Cross-Platform Reverse Engineering of CAN Bus Commands from Mobile Apps, ISOC Network and Distributed System Security Symposium (NDSS) 2020. *(acceptance rate 18.3% = 73/399)*.

C34. **[ICSE'20]** Joshua Garcia, Yang Feng, Junjie Shen, Sumaya Almanee, Yuan Xia, and **Qi Alfred Chen**, A Comprehensive Study of Autonomous Vehicle Bugs, International Conference on Software Engineering (ICSE) 2020. *(acceptance rate 23.5% = 129/550)*.

C33. **[ICLR'20]** Yunhan Jia, Yantao Lu, Junjie Shen, **Qi Alfred Chen**, Hao Chen, Zhenyu Zhong, and Tao Wei, Fooling Detection Alone is Not Enough: Adversarial Attack against Multiple Object Tracking, International Conference on Learning Representations (ICLR) 2020. *(acceptance rate 26.5% = 687/2594)*.

C32. **[TRB'20]** Shihong Huang, Wai Wong, Yiheng Feng, **Qi Alfred Chen**, Henry X. Liu, and Z. Morley Mao, Cyber-Vulnerability Analysis for Connected Vehicle Based Traffic Signal Control Systems, Transportation Research Board Annual Meeting (TRB) 2020.

C31. **[EuroSys'20]** Liangyi Gong, Zhenhua Li, Feng Qian, Zifan Zhang, **Qi Alfred Chen**, Zhiyun Qian, Yunhao Liu, Experiences of Landing Machine Learning onto Market-Scale Mobile Malware Detection, European Systems Conference (EuroSys) 2020. *(acceptance rate 18.4%=43/234)*

C30. [EuroS&P'20] David Ke Hong, John Kloosterman, Yuqi Jin, Yulong Cao, **Qi Alfred Chen**, Scott Mahlke, and Z. Morley Mao, AVGuardian: Detecting and Mitigating Publish-Subscribe Overprivilege for Autonomous Vehicle Systems, IEEE European Symposium on Security and Privacy (EuroS&P) 2020. *(acceptance rate 14.6%=38/261)*

C29. [AutoSec'20] Shengtuo Hu, **Qi Alfred Chen**, Jiwon Joung, Can Carlak, Yiheng Feng, Z. Morley Mao, and Henry X. Liu, CVShield: Guarding Sensor Data in Connected Vehicle withTrusted Execution Environment, ACM CODASPY Workshop on Automotive and Aerial Vehicle Security (AutoSec) 2020.

C28. **[CCS'19]** Zhenyuan Li, **Qi Alfred Chen**, Chunlin Xiong, Yan Chen, Tiantian Zhu, and Hai Yang, Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts, ACM Conference on Computer and Communications Security (CCS) 2019. *(acceptance rate 16.0% = 149/933)*.

C27. **[CCS'19]** Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, **Qi Alfred Chen**, Kevin Fu, and Z. Morley Mao, Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving, ACM Conference on Computer and Communications Security (CCS) 2019. *(acceptance rate 16.0% = 149/933)*.

C26. **[MobiSys'19]** Fan Dang, Zhenhua Li, Yunhao Liu, Ennan Zhai, **Qi Alfred Chen**, Tianyin Xu, Yan Chen, and Jingyu Yang, Understanding Fileless Attacks on Linux-based IoT Devices with HoneyCloud, ACM International Conference on Mobile Systems, Applications, and Services (MobiSys) 2019. *(acceptance rate 22.7% = 39/172)*

C25. **[MobiSys'19]** Yuxuan Yan, Zhenhua Li, **Qi Alfred Chen**, Christo Wilson, Tianyin Xu, Ennan Zhai, Yong Li, and Yunhao Liu, Understanding and Detecting Overlay-based Android Malware at Market Scales, ACM International Conference on Mobile Systems, Applications, and Services (MobiSys) 2019. *(acceptance rate 22.7% = 39/172)*

C24. **[TRB'19]** Wai Wong, Shihong Huang, Yiheng Feng, **Qi Alfred Chen**, Henry X. Liu, and Z. Morley Mao, Trajectory-Based Hierarchical Defense Model to Detect Cyber-Attacks on Transportation Infrastructure, Transportation Research Board 2019 Annual Meeting (TRB), 2019.

C23. **[NDSS'18] Qi Alfred Chen**, Yucheng Yin, Yiheng Feng, Z. Morley Mao, and Henry X. Liu, Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control, ISOC Network and Distributed System Security Symposium (NDSS) 2018. *(acceptance rate 21.5% = 71/331)*

C22. **[TRB'18]** Yiheng Feng, Shihong Huang, **Qi Alfred Chen**, Henry X. Liu, and Z. Morley Mao, Vulnerability of Traffic Control System Under Cyber-Attacks Using Falsified Data, Transportation Research Board Annual Meeting (TRB) 2018. *(selected for journal publication with acceptance rate 20.0%)*

C21. [SEC'18] Ashkan Nikravesh, **Qi Alfred Chen**, Scott Haseley, Xiao Zhu, Geoffrey Challen, and Z. Morley Mao, QoE Inference and Improvement Without End-Host Control, ACM/IEEE Symposium on Edge Computing (SEC), 2018.

C20. [AsiaCCS'18] Jeremy Erickson, **Qi Alfred Chen**, Xiaochen Yu, Erinjen Lin, Robert Levy, and Z. Morley Mao, No One In The Middle: Enabling Network Access Control Via Transparent Attribution, ACM ASIA Conference on Computer and Communications Security (AsiaCCS), 2018. *(acceptance rate 20.0%)*

C19. **[CCS'17] Qi Alfred Chen**, Matthew Thomas, Eric Osterweil, Yulong Cao, Jie You, Z. Morley Mao, Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study, ACM Conference on Computer and Communications Security (CCS) 2017. *(acceptance rate 18.1% = 151/836)*

C18. **[IV'17]** Yunhan Jack Jia, Ding Zhao, **Qi Alfred Chen**, Z. Morley Mao, Towards Secure and Safe Appified Automated Vehicles, IEEE Intelligent Vehicles Symposium (IV) 2017. *(selected for oral presentation with acceptance rate 10.0%)*

C17. **[NDSS'17]** Yunhan Jack Jia, **Qi Alfred Chen**, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Z. Morley Mao, and Atul Prakash, ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms, ISOC Network and Distributed System Security Symposium (NDSS) 2017. *(acceptance rate 16.0% = 68/423)*

C16. [EuroS&P'17] Yunhan Jack Jia, **Qi Alfred Chen**, Yikai Lin, Chao Kong, and Z. Morley Mao, Open Doors for Bob and Mallory: Open Port Usage in Android Apps and Security Implications, IEEE European Symposium on Security and Privacy (EuroS&P), 2017. *(acceptance rate 19.6% = 38/194)*

C15. [FEAST'17] David Ke Hong, **Qi Alfred Chen**, Z. Morley Mao, An Initial Investigation of Protocol Customization, ACM CCS Workshop on Forming an Ecosystem Around Software Transformation (FEAST), 2017.

C14. **[S&P'16] Qi Alfred Chen**, Eric Osterweil, Matthew Thomas, and Z. Morley Mao, MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era, IEEE Symposium on Security and Privacy (S&P) 2016. *(acceptance rate 13.3% = 55/413)*

C13. **[IMC'16]** Yihua Guo, Feng Qian, **Qi Alfred Chen**, Z. Morley Mao, and Subhabrata Sen, Understanding On-device Bufferbloat for Cellular Upload, ACM SIGCOMM Internet Measurement Conference (IMC) 2016. *(acceptance rate 25.3% = 46/182)*

C12. **[NDSS'16]** Yuru Shao, Jason Ott, **Qi Alfred Chen**, Zhiyun Qian, and Z. Morley Mao, Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework, ISOC Network and Distributed System Security Symposium (NDSS) 2016. *(acceptance rate 15.4% = 60/389)*

C11. [FC'16] Earlence Fernandes, **Qi Alfred Chen**, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash, Android UI Deception Revisited: Attacks and Defenses, International Conference on Financial Cryptography and Data Security (FC), 2016. *(acceptance rate 26.0%)*

C10. [Internet-QoE'16] Ashkan Nikravesh, David Ke Hong, **Qi Alfred Chen**, Harsha V. Madhyastha, and Z. Morley Mao, QoE Inference Without Application Control, ACM SIGCOMM Workshop on QoE-based Analysis and Management of Data Communication Networks (Internet-QoE), 2016.

C9. **[CCS'15] Qi Alfred Chen**, Zhiyun Qian, Yunhan Jia, Yuru Shao, and Z. Morley Mao, Static Detection of Packet Injection Vulnerabilities – A Case for Identifying Attacker-controlled Implicit Information Leaks, ACM Conference on Computer and Communications Security (CCS) 2015. *(acceptance rate 19.8% = 128/646)*

C8. **[Mobicom'15]** Yunhan Jack Jia, **Qi Alfred Chen**, Z. Morley Mao, Jie Hui, Kranthi Sontineni, Alex Yoon, Samson Kwong, and Kevin Lau, Performance Characterization and Call Reliability Problem Diagnosis for Voice over LTE, ACM Annual International Conference on Mobile Computing and Networking (Mobicom) 2015. *(acceptance rate 18.4% = 38/207)*

C7. **[USENIX Security'14] Qi Alfred Chen**, Zhiyun Qian, and Z. Morley Mao, Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks, USENIX Security Symposium 2014. *(acceptance rate 19.0% = 67/352)*

C6. **[IMC'14] Qi Alfred Chen**, Haokun Luo, Sanae Rosen, Z. Morley Mao, Karthik Iyer, Jie Hui, Kranthi Sontineni, and Kevin Lau, QoE Doctor: Diagnosing Mobile App QoE with Automated UI Control and Cross-layer Analysis, ACM SIGCOMM Internet Measurement Conference (IMC) 2014. *(acceptance rate 22.9% = 43/188)*

C5. **[Mobicom'14]** Sanae Rosen, Haokun Luo, **Qi Alfred Chen**, Z. Morley Mao, Jie Hui, Aaron Drake, and Kevin Lau, Discovering Fine-grained RRC State Dynamics and Performance Impacts in Cellular Networks, ACM Annual International Conference on Mobile Computing and Networking (Mobicom) 2014. *(acceptance rate 16.4% = 36/220)*

C4. [S3'14] Sanae Rosen, Haokun Luo, **Qi Alfred Chen**, Z. Morley Mao, Jie Hui, Aaron Drake, and Kevin Lau, Understanding RRC State Dynamics Through Client Measurements with Mobilyzer, ACM MobiCom Workshop on Wireless of the Students, by the Students, and for the Students (S3), 2014.

C3. [WCNC'14] Yu Stephanie Sun, Lei Xie, **Qi Alfred Chen**, Sanglu Lu, and Daoxu Chen, Efficient Route Guidance in Vehicular Wireless Networks, IEEE Wireless Communications and Networking Conference (WCNC), 2014.

C2. [DASC'11] **Qi Chen**, Wenmin Lin, Shui Yu, and Wanchun Dou, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), 2011.

C1. [WISM'11] Rutao Yang, **Qi Chen**, Lianyong Qi, and Wanchun Dou, A QoS Evaluation Method for Personalized Service Requests, International Conference on Web Information Systems and Mining, 2011.

Journal Publications

(top-tier journals are highlighted in **bold**)

J10. **[TSE]** Yuqi Huai, Sumaya Almanee, Yuntianyi Chen, Xiafa Wu, **Qi Alfred Chen**, and Joshua Garcia, scenoRITA: Generating Diverse, Fully-Mutable, Test Scenarios for Autonomous Vehicle Planning, IEEE Transactions on Software Engineering (TSE) 2023. *(Indexed by SCI, Impact Factor 7.4)*

J9. [FTEDA] Qi Zhu, Bo Yu, Ziran Wang, Jie Tang, **Qi Alfred Chen**, Zihao Li, Xiangguo Liu, Yunpeng Luo and Lingzi Tu, Cloud and Edge Computing for Connected and Automated Vehicles, Foundations and Trends in Electronic Design Automation 2023.

J8. **[T-ITS]** Zhen Yang, Jun Ying, Junjie Shen, Yiheng Feng, **Qi Alfred Chen**, Z. Morley Mao, and Henry X. Liu, Anomaly Detection Against GPS Spoofing Attacks on Connected and Autonomous Vehicles Using Learning from Demonstration, IEEE Transactions on Intelligent Transportation Systems (T-ITS) 2023. *(Indexed by SCI, Impact Factor 6.492)*

J7. **[T-ITS]** Yiheng Feng, Shihong Huang, Wai Wong, **Qi Alfred Chen**, Z. Morley Mao, and Henry X. Liu, On the Cybersecurity of Traffic Signal Control System with Connected Vehicles, IEEE Transactions on Intelligent Transportation Systems (T-ITS) 2022. *(Indexed by SCI, Impact Factor 6.492)*

J6. [Computers & Security] Zhenyuan Li, **Qi Alfred Chen**, Runqing Yang, Yan Chen, Wei Ruan, Threat Detection and Investigation with System-level Provenance Graphs: A Survey, Computers & Security 2021. *(Indexed by SCI, Impact Factor 3.579)*

J5. [IJIS] Tong Chen, Jiqiang Liu, Yingxiao Xiang, Wenjia Niu, Endong Tong, Shuoru Wang, He Li, Liang Chang, Gang Li, and **Qi Alfred Chen**, Adversarial Retraining Attack of Asynchronous Advantage Actor-Critic Based Pathfinding, International Journal of Intelligent Systems 2021. *(Indexed by SCI, Impact Factor 8.709)*

J4. [JCST] Endong Tong, Jiqiang Liu, Wenjia Niu, Liang Chang, **Qi Alfred Chen**, and Gang Li, Robustness Assessment of Asynchronous Advantage Actor-Critic based on Dynamic Skewness and Sparseness Computation: A Parallel Computing View, Journal of Computer Science and Technology 2021. *(Indexed by SCI, Impact Factor 1.506)*

J3. [SCN] Yunzhe Tian, Jiqiang Liu, Endong Tong, Wenjia Niu, Liang Chang, **Qi Alfred Chen**, Gang Li, and Wei Wang, Towards Revealing Parallel Adversarial Attack on Politician Socialnet of Graph Structure, Security and Communication Networks 2021. *(Indexed by SCI, Impact Factor 1.288)*

J2. **[TRR]** Yiheng Feng, Shihong Huang, **Qi Alfred Chen**, Henry X. Liu, and Z. Morley Mao, Vulnerability of Traffic Control System Under Cyberattacks with Falsified Data, Transportation Research Record (TRR), Volume 2672, Issue 1, Page 1-11, March 2018. *(Indexed by SCI, Impact Factor 0.695)*

J1. [FGCS] Wanchun Dou, **Qi Chen**, and Jinjun Chen, A Confidence-Based Filtering Method for DDoS Attack Defense in Cloud Environment, Future Generation Computer Systems (FGCS), Volume 29, Issue 7, Pages 1838-1850, September 2013. *(Indexed by SCI, Impact Factor 4.787)*

RESEARCH IMPACTS

Selected Media Coverage

- Armed with Traffic Cones, Protesters are Immobilizing Driverless Cars, ***NPR (National Public Radio)***, 8/26/2023.
- Autonomous Vehicles Can Be Tricked into Dangerous Driving Behavior, ***ACM TechNews*** & ***CPS-VO***, 06/02/2022
- Autonomous Vehicles can be Tricked into Erratic Driving Behavior, *Help Net Security*, 06/02/2022
- The Risks Posed by Wireless Automotive Dongles, *Data Beach Today*, 08/12/2020
- Five Components Of Autonomous Car Security, ***Forbes***, 10/31/2019
- Apps Available for Your Smartphone Could Steal Your Personal Information, *WXYZ-TV (**ABC** afflicated)*, 06/28/2017
- An Obsure App Flaw Creates Backdoors in Millions of Smartphones, ***Wired***, 04/28/2017
- US-CERT: Leaked WPAD Queries Could Expose Corporate to MitM Attacks, *SecurityAffairs*, 05/26/2016
- When Domain Names Attack: the WPAD Name Collision Vulnerability, *NakedSecurity*, 05/25/2016
- Android Attack Improves Timing, Allows Data Theft, ***Ars Technica***, 08/24/2014
- Gmail Smartphone App Hacked by Researchers, ***BBC News***, 08/22/2014
- Researchers Find Way to Hack Gmail with 92 Percent Success Rate, ***CNET News***, 08/21/2014
- New Hack Could Steal Personal Information from Gmail, Other Popular Apps, *CBS News*, 08/21/2014
- Sneak Attack: Android Apps Can Spy on Each Other, *NBC News*, 08/21/2014

Selected Vulnerability Disclosures

- **USDHS US-CERT Alert TA16-144A**: WPAD Name Collision Vulnerability
- CVE-2022-48198, CVE-2022-48217: Name-from-parameter vulnerabilities found in ROS repositories `ntpd_driver` and `tf_remapper_cpp`
- CVE-2019-19320, CVE-2019-19321, CVE-2019-19322, CVE-2019-19323: Authentication vulnerabilities in various wireless OBD-II dongles such as Carly, LELink, FIXD, Carista, etc.
- CVE-2016-3898: Privilege escalation vulnerability in Android Telephony service
- CVE-2016-5227: Device authentication hijacking vulnerability in AirDroid
- AndroidID-21669196, AndroidID-22541289, AndroidID-24776299, AndroidID-23782371: Privilege escalation vulnerability in Android Short Message Service (SMS), NSD, GPS, and Telephony and Telecomm services

Selected Industry Discussions & Responses

- Triggered **over 30 Autonomous Driving (AD) companies** such as Tesla, GM, Daimler, Baidu, TuSimple, Aptiv, Hyundai, Volkswagen, Bosch, Lyft, Nuro, Toyota, Hyundai, Kia, and Volvo to start investigating our newly-discovered security vulnerabilities in AD localization and/or perception algorithms; some confirmed to work on fixes.
- Acknowledgments from **IEEE 1609 WG (V2X standardization working group)** for 4 newly-discovered P2PCD protocol vulnerabilities; mitigation solutions *planned to be integrated into the next version of IEEE 1609.2*.
- Invited to perform vulnerability disclosure at **Auto-ISAC (Automotive Information Sharing & Analysis Center)**, which has *50+ company members* including light- and heavy-duty vehicle OEMs, suppliers and the commercial vehicle sector.

- Triggered the security update to restrict /proc/PID access in **Android** ("Honey, I Shrunk the Attack Surface" from Nick Kralevich, Android Platform Security Engineering Lead, at Black Hat USA 2017)
- Email acknowledgements from **Apple, Microsoft and Comcast** on the reported client-side name collision vulnerabilities
- RIPE 72 discussion, 05/23/2016: *Alert (TA16-144A) WPAD Name Collision Vulnerability*
- Verisign's remediation suggestions: *White Paper: Enterprise Remediation for WPAD Name Collision Vulnerability*

Research Artifacts

We open-source the artifacts from the research in my group as much as possible at the official group GitHub https://github.com/ASGuard-UCI to benefit the community. Recent examples include:

- PlanFuzz (Published at NDSS'22): Released the source code of the PlanFuzz tool and the evaluation scenario setup at https://github.com/ASGuard-UCI/PlanFuzz.
- ld-metric (Published at CVPR'22): Released the source code of the new metric calculation and the evaluation setup at https://github.com/ASGuard-UCI/ld-metric
- MSF-ADV (Published at IEEE S&P'21): Released the MSF-ADV attack generation code, evaluation data, and also the generated adversarial 3D meshes from our experiments at https://github.com/ASGuard-UCI/MSF-ADV
- DRP-attack (Published at Usenix Security'21): Released the DRP attack generation code and evaluation data at https://github.com/ASGuard-UCI/DRP-attack, and also released our instrumented simulation setup that can bridge LGSVL with a production lane keeping system (spent months to develop) at https://github.com/ASGuard-UCI/openpilot.

Funding

Total: $14,716,284, My share: $2,252,741:

- US Department of Transportation (USDOT), "CARMEN+: Center for Automated Vehicle Research with Multimodal AssurEd Navigation," Total: $10,000,000 (11/15/2022 – 11/30/2028). Role: Co-PI. **My share: $450,000**.
- NSF (National Science Foundation), "CAREER: Securing the AI Stack in Autonomous CPS under Physical-Layer Attacks: A Systems Perspective," Total: $523,402 (7/01/2022 – 6/30/2027). Role: Single PI. **My share: $523,402**.
- Toyota Motor North America (TMNA) Research Gift, "Autonomy Stack AI Security", Total: $70,000 (2022). Role: Single PI. **My share: $70,000**.
- Qualcomm Research Gift, "V2X Security Research", Total: $75,000 (2022). Role: Single PI. **My share: $75,000**.
- General Motors (GM) Research Gift, "Adversarial Automotive AI Research", Total: $100,000 (2021). Role: Single PI. **My share: $100,000**.
- Toyota Motor North America (TMNA) Research Gift, "Autonomy Stack Defensive Security", Total: $70,000 (2021). Role: Single PI. **My share: $70,000**.
- US Department of Transportation (USDOT), "Assured Navigation and Timing Engineering for Automated Transportation Education and Research – DOT Tier 1 University Transportation Center (UTC)," Total: $1,925,000 (10/01/2020 – 9/30/2022). Role: Co-PI. **My share: $99,755**.
- NSF (National Science Foundation), "CPS: Small: Collaborative Research: SecureNN: Design of Secured Autonomous Cyber-Physical Systems against Adversarial Machine Learning Attacks," Total: $500,000 (11/01/2019 – 10/31/2022). Role: Lead PI. **My share: $249,998**.
- NSF (National Science Foundation), "SaTC: TTP: Medium: Collaborative: Exposing and Mitigating Security/Safety Concerns of CAVs: A Holistic and Realistic Security Testing Platform for Emerging CAVs," Total: $1,200,000 (10/01/2019 – 9/30/2023). Role: Lead PI. **My share: $374,204**.
- NSF (National Science Foundation), "CRII: SaTC: Automated Security Analysis of Software-Based Control in Emerging Smart Transportation Under Sensor Attacks," Total: $174,997 (04/01/2019 – 03/31/2021). Role: Single PI. **My share: $174,997**.

Student Mentoring Experience

(under-represented minority (URM) students in CS/STEM are denoted with *)

Graduate Students Mentoring (Total: 7 Ph.D. (2 URM), 9 M.S. (2 URM))

- Takami Sato (UCI M.S., 2018/10–2019/9, UCI Ph.D., 2019/9–): AI security in CPS.
  - Publications: Usenix Security'21 (co-1st author), CVPR'22 (1st author), NDSS'24 (1st author), ICCV'23 (a), ICCV'23 (b), IROS'23, IV'21.

  - Awards: **NDSS'20 Best Technical Poster Award** (*top 1/30*), **Public Impact Fellowship** (*top 15 students across all schools*), **Graduate Dean's Dissertation Fellowship Award** (*top 1-2 students per school*), **Beall Family Foundation Graduate Student Entrepreneur Award in Computer Science**.
- Ningfei Wang (UCI Ph.D., 2019/9–): : AI security in CPS.
  - Publications: IEEE S&P'21 (co-1st author), ICCV'23 (1st author), Usenix Security'21.
  - Awards: **Dean's Fellowship** (*top 10 in CS*), **NDSS'20 Best Technical Poster Award** (*top 1/30*), **Embedded and/or Cyber-Physical System (ECPS) Fellowship** (*top 2 in CS*), **ICS Innovation Endowed Fellowship**, **Beall Family Foundation Graduate Student Entrepreneur Award in Computer Science**.
- Ziwen Wan (UCI Ph.D., 2019/9–): AI safety/security in CPS.
  - Publications: NDSS'22 (1st author), ICSE'23, IROS'23, IV'23.
- Fayzah Alshammari* (UCI Ph.D., 2022/9–): Cybersecurity in autonomous systems.
- Junjie Shen (UCI Ph.D., 2018/7–2022/7): AI security in CPS.
  - Publications: Usenix Security'20 (1st author), Usenix Security'21 (co-1st author), IROS'23 (1st author), IV'23 (1st author), NDSS'22, IV'21, ICSE'20, ICLR'20.
  - Awards: **NDSS'19 Distinguished Poster Presentation Award** (*top 2/36*), **NDSS'20 Best Technical Poster Award** (*top 1/30*), **Graduate Dean's Dissertation Fellowship** (*top 1-2 students per school*), **Beall Family Foundation Graduate Student Entrepreneur Award in CS**.
  - First job: Research Scientist at Meta.
- M.S. Keystone Project (UCI, 2023/4–2023/7, faculty advisor): Pallavi Garg*, Nitesh Gupta, Aditya Sanjay Dikshit, and Shubham Bhanudas Abhale.
- M.S. students mentoring: Jun Yeon Won (UCI M.S., 2018/07–2019/07, now OSU Ph.D., **NDSS'19 Distinguished Poster Presentation Award**), Jong Ho Lee (UCI M.S., 2018/10–2019/09, now U Maryland PhD), Siddhant Mahesh Deshpande (UCI M.S., 2023/07–), Vyshnavi Kurella* (UCI M.S., 2023/07–).

Undergraduate Students Mentoring (Total: 32 B.S. (8 URM))

- Kanglan Tang* (UCI B.S., 2019/12–2021/08, now UC Berkeley M.S.).
  - Publications: AutoSec'21 (1st author), SafeThings'21 Demo (1st author).
  - Awards: **NDSS'21 Student Travel Grant**, **2021 Chancellor's Award for Excellence in Undergraduate Research** (*one per school*).
- Rong Mu* (UCI B.S., 2022/07–).
  - Awards: **2023 Chancellor's Award for Excellence in Undergraduate Research** (*one per school*), **ICS Outstanding Contribution to Research Undergraduate Award** (*top 10 per school*), **3rd place Award in the UROP Poster Presentation**.
- Nanze Chen (UCI B.S., 2022/10–2023/09, will be U of Cambridge M.S.).
  - Awards: **ICS Outstanding Contribution to Research Undergraduate Award** (*top 10 per school*).
- Zeyuan Chen (UCI B.S., 2019/09–2020/07, now CMU M.S.). *Publications: Usenix Security'20.*
- Christopher Joseph Dipalma (UCI B.S., 2019/09–2021/09, now at Intel). *Publications: AutoSec'21 Demo (1st author), SafeThings'21 Demo (1st author).*
- Undergraduate Senior Design Project (UCI, 2019/9–2020/3, faculty advisor): Christopher Joseph Dipalma, Tong Ray Huang, Sammy Li Wong, David Dang Khoi Pham.
- Undergraduate Multi-Disciplinary Design Program (UMich, Winter 2016, student mentor): Yidan Zhang*, Chia-Yen Lee*, Jinting Hayter*, Lihui Qin*, Abigail Grobbel*.
- Others: Yuan Xia* (UCI BS, 2019/01–2020/06, Now USC MS), Newman Cheng (UCI BS, 2018/10–2020/07, now Columbia MS), Kyle Bartz (UCI BS, 2018/09–2019/07, now in Amazon), Hongyu Chen* (UCI BS, 2021/09–2022/06, Now UCI MS), Chen Wang (UCI BS, 2019/10–12, now UC Berkeley MS), Huilai Liu (UCI BS, 2020/01–09, now UCI MS), Artur Gharibkhanyan (UCI BS, 2019/09–11, now at Glenair), Lei Ruan (Tsinghua BS, now CWRU MS), Aryan Jain (IIT Delhi BS, 2022/7–2022/9), Justin Yue (UCI BS, 2022/05–), Jalen Chuang (UCI BS, 2020/02–), Joseph Wong (UCI BS, 2021/05–), Jiahao Chen (UCI BS, 2021/05–), Han Wang (UCI BS, 2021/05–2022/07, now UPenn MS), Haonan Xu (UCI BS, 2020/02–09), Liangze Yu (UCI BS, 2019/01–07), Wentao Chen (UCI BS, 2023/01–), Chi Zhang (UCI BS, 2023/01–), Sam Der (UCI BS, 2023/01–).

TEACHING EXPERIENCE

- Instructor, CS 134 Computer and Network Security, UC Irvine, Fall 2019-2022
  - Undergraduate-level course on foundational work and current topics in cryptography and network security.
  - Evaluation highlights: Always **over 70%** students "Agree" or "strongly agree" that "the instructor presented the course material in a way that helped me to understand it." and "I feel that the instructor provided opportunities for learning that helped me to better understand the course material."
  - Student quotes:
    - "*I think the professor was able to break down difficult topics into small and understandable parts.*"
    - "*[Homeworks and lectures] is just the right amount of work and thinking required.*"
    - "*[Homeworks] did stretch us and prepare us for the midterm, so though very difficult, they were valuable.*"

- Instructor, CS 205 Computer Systems Security, UC Irvine, Spring 2019-2023
  - **New course** designed by me, already became a **core course** in the CS MS and PhD programs
  - Graduate-level course on foundational work and current topics in computer and network security.
  - Evaluation highlights: Always **over 80%** students "strongly agree" that "this course broadened my perspective" and "the instructor presented the course material in a way that helped me to understand it."
  - Student quotes:
    - "*The best point about Alfred is that he tried to teach us how to think critically.*"
    - "*It was interesting to read recent research topics in computer security and I learned a lot, especially how to think critically while reading a research paper.*"
    - "*Help me a lot about understanding the paper and how to read the paper in a proper way.*"

- Instructor, Osher Lifelong Learning Institute (OLLI), Fall 2017
  - Course: "How to Use Your Smartphone Securely? Technology and Security of Smart Devices and Smart Systems".
  - 5 two-hour classes each semester on the technology and security issues of smart devices and smart systems.
  - Quote from course evaluator Mr. Sydney Kaufman:
    - "*The group participation and interest was far above our norm at OLLI. You should give some thought to teaching at least as an avocation once you get your degree.*"

- Guest lecturer
  - 10/22/2020: EECS 588 Computer and Network Security, U of Michigan
  - 06/01/2021: SWE 266P Software Security and Dependability, UC Irvine
  - 05/03/2022: SWE 266P Software Security and Dependability, UC Irvine
  - 02/15/2023: EECS 231 Advanced System Security, UC Irvine
  - 05/25/2023: SWE 266P Software Security and Dependability, UC Irvine

SELECTED TALKS

- On the Cyber-Physical Security of Latest Autonomous Driving and Intelligent Transportation Systems
  – 10/07/2022: Invited talk at Workshop on Safety Validation of Connected and Automated Vehicles at IEEE ITSC'22
  – 11/30/2022: Vehicle Research and Test Center (VRTC), National Highway Traffic Safety Administration (NHTSA)
  – 02/20/2023: Invited talk at UCI-IPN Binational Scientific Research Symposium 2023
  – 05/11/2023: **Keynote** at AUTOSAR Open Conference 2023
  – 05/19/2023: **Keynote** at 5th Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT) at ICSE'23

- On the Semantic AI Security in CPS: The Case of Autonomous Driving
  (Variants: Towards Secure & Safe Data-Driven Decision Making in AI-Enabled Autonomous Cyber-Physical Systems)
  – 03/28/2022: Department of Electrical and Computer Engineering (ECE), UC Riverside
  – 03/29/2022: Department of Electrical and Computer Engineering (ECE), UCLA
  – 05/24/2022: Short talk, IEEE S&P'22
  – 06/22/2022: Korea Institute of Information Security & Cryptology (KIISC) Advances in Computer Security school
  – 06/26/2022: **Keynote** at Dependable and Secure Machine Learning (DSML) workshop, co-located with DSN'22
  – 07/18/2022: Breakout: Cybersecurity Hot Topics, Automated Road Transportation Symposium (ARTS)
  – 08/02/2022: Seminar on Challenges & Opportunties on Security & Privacy in Machine Learning
  – 08/29/2022: Zhejiang University (ZJU) CSE Summer School
  – 08/30/2022: INFORMS Conference on Security (IConS)

– 11/15/2022: Johns Hopkins University (JHU) Institute for Assured Autonomy (IAA)
– 03/13/2023: Halıcıoğlu Data Science Institute (HDSI), UCSD

- Cyber-Attacks against AI Stack in Autonomous Driving & Intelligent Transportation
  – 06/24/2022: 2nd IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS)

- Towards Secure and Robust AI Stack in Autonomous Driving
  (Variants: Towards Secure and Robust AI Stack in Emerging Autonomous Cyber-Physical System, Towards Secure and Robust Autonomy Software in Autonomous Driving (and Smart Transportation))
  – 09/10/2020: General Motors (GM) Research, USA
  – 09/22/2020: Auto-ISAC (Automotive Information Sharing & Analysis Center)
  – 09/24/2020: Baidu Security Lab (X-Lab), USA
  – 10/02/2020 (Part 1): IBM T.J. Watson Research Center
  – 10/12/2020: Department of Computer Science, Duke University
  – 10/17/2020: Annual Convention of CIE (Chinese Institute of Engineers), USA
  – 11/20/2020 (Part 2): IBM T.J. Watson Research Center
  – 12/08/2020: Transportation Workshop, Duke-NCSU-UNC Statistical & Applied Math Sciences Institute (SAMSI)
  – 12/29/2020: Baidu Intelligent Driving Group (IDG)
  – 02/11/2021: InfoTechnology Center, Toyota Motor North America (TMNA)
  – 02/24/2021: NIO Security Research, USA
  – 06/07/2021: **Keynote** at 7th ACM Cyber-Physical System Security Workshop (CPSS'21), co-located with ACM AsiaCCS'21
  – 09/10/2021: School of Computing and Informatics, University of Louisiana at Lafayette (ULL)
  – 09/19/2021: 2nd Workshop on Internet of Things in Intelligent Transportation Systems: Opportunities and Challenges (IoT-in-ITS), co-located with ITSC'21
  – 10/11/2021: Department of Computer Science and Engineering, Ohio State University (OSU)
  – 10/13/2021: **5th Annual Auto-ISAC Cybersecurity Summit**, GM Marriott at the Renaissance Center, Detroit (the ***only*** invited speaker on related academic research)
  – 10/24/2021: **Keynote** at 1st International Workshop on Reliability of Advanced Driving Assistant Systems (RADAS'21), co-loated with ISSRE'21
  – 11/19/2021: Workshop on Future Automotive Research Datasets, Oak Ridge National Laboratory (ORNL)
  – 12/09/2021: DiDi Autonomous Driving, USA
  – 02/15/2022: Qualcomm Technologies, USA
  – 04/06/2022: University of Texas at Dallas
  – 11/18/2022: NVIDIA

- Ghost Cars & Fake Obstacles: First Look at Control Software Stack Security in Emerging Smart Transportation
  – 08/13/2019: 2019 USENIX Summit on Hot Topics in Security (HotSec'19), in conjuction with USENIX Security 2019, Santa Clara (**Most Amusing Award** & **Most Engaging Award**)

- Tutorial: Initial Explorations of Software Security in Connected and Automated Vehicles
  – 03/27/2019: 1st ACM Workshop on Automotive Cybersecurity (AutoSec'19), in conjuction with ACM CODASPY 2019, Dallas

- Ghost Cars and Fake Obstacles: Automated Security Analysis of Emerging Smart Transportation Systems
  – 09/28/2018: CS Seminar Series, UCI Department of Computer Science
  – 01/16/2019: 2nd Annual Irvine Symposium on Emerging Research in Transportation (ISERT'19), UCI Institute of Transportation Studies (ITS)
  – 03/22/2019: ITS Seminar Series, UCI Institute of Transportation Studies (ITS)
  – 03/29/2019: Emerging Scholars Transportation Research Symposium (ESTRS), USC METRANS Transportation Center
  – 04/10/2019: METRANS 2019 Speaker Series, USC METRANS Transportation Center
  – 05/14/2019: IoT Security & Privacy Conference and Research Symposium, UCI Cybersecurity Policy & Research Institute (CPRI) & Institute for Software Research (ISR)
  – 06/10/2019: UCI/UCR/UPHF 1st International Workshop on Cyber-Physical Systems and their Applications in Intelligent and Connected Transportation System, UCI Center for Embedded and Cyber-physical Systems (CECS)

- Securing Smart, Connected Systems through Systematic Problem Analysis and Mitigation
  – 02/15/2018: Department of Computer Science & Engineering and Department of Electrical & Computer Engineering, Texas A&M University
  – 02/26/2018: Department of Computer Science & Engineering, Washington University in St. Louis

– 03/01/2018: Department of Electrical & Computer Engineering, Boston University
– 03/13/2018: Department of Computer Engineering, UC Santa Cruz
– 03/15/2018: Department of Computer Science, UC Irvine
– 03/20/2018: Department of Electrical & Computer Engineering, New York University
– 03/22/2018: Department of Computer Science, University of Arizona
– 03/29/2018: Department of Computer Science, University of Virginia
– 04/02/2018: Department of Electrical & Computer Engineering, Northeastern University
– 04/05/2018: Department of Computer Science, University of Pittsburgh
– 04/10/2018: Department of Computer Science, Georgia Institute of Technology
– 04/13/2018: Department of Computer Science & Engineering, University of Minnesota Twin Cities

- Security Analysis of Next-generation Connected Vehicle based Transportation
  – 10/20/2017: Mcity Cybersecurity meeting, University of Michigan Transportation Research Institute (UMTRI)
  – 11/03/2017: Short talk, 2019 ACM Workshop on Forming an Ecosystem Around Software Transformation (FEAST'19), in conjuction with ACM CCS 2017, Dallas

- MitM, Code Injection, Cred Theft, and More Found at the Scene of a Name Collision
  – 09/12/2017: Tsinghua University, China
  – 09/15/2017: Nanjing University, China
  – 11/01/2017: 24th ACM Conference on Computer and Communications Security (CCS'17), Dallas

- MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era
  – 05/25/2016: 37th IEEE Symposium on Security and Privacy (S&P'16), San Jose
  – 11/04/2016: CSE Research Honors Competition, University of Michigan

- Static Detection of Packet Injection Vulnerabilities: A Case for Identifying Attacker-controlled Implicit Information Leaks
  – 10/13/2015: 22nd ACM Conference on Computer and Communications Security (CCS'15), Denver
  – 11/06/ 2015: CSE Research Honors Competition, University of Michigan

- Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks
  – 07/10/2014: Nanjing University, China
  – 08/22/2014: 23rd USENIX Security Symposium (USENIX Security'14), San Diego

ACADEMIC SERVICES

(top-tier venues are highlighted in **bold**)

- ***Founder***: ISOC Symposium on Vehicle Security & Privacy (VehicleSec) (2023, leading co-founder, ***first*** *academic conference dedicated to vehicle security and privacy*, co-located w/ **NDSS'23**)

- ***Founder***: ACM/ISOC AutoSec (Automotive & Autonomous Vehicle Security) Workshop (2019, leading co-founder, co-located w/ ACM CODASPY'19-20 and then textbfNDSS'21-22)

- ***Founder***: AutoDriving CTF (Capture-The-Flag) Contest at DEF CON (2021, leading co-creator, *DEF CON's* ***first*** *autonomous driving-themed hacking event*; DEF CON is one of world's largest & most notable hacker conventions)

- General Chair: VehicleSec 2023 (co-located w/ **NDSS'23**), ACM/ISOC AutoSec (Automotive & Autonomous Vehicle Security) Workshop 2019-22 (co-located w/ **NDSS'21-22**, ACM CODASPY'19-20), IEEE SafeThings Workshop 2021 (co-located w/ IEEE S&P'21).

- Organizer: **AutoDriving CTF (Capture-The-Flag) Contest at DEF CON** 2021-23.

- PC member (selected): **IEEE S&P 2024**, **Usenix Security 2021-2023**, **ISOC NDSS 2022-2023**, **ACM CCS 2021, 2023**, **CVPR 2022-2023**, **ECCV 2022**, **NeurIPS 2023**, **ICRA 2023**, **IROS 2023**, **INFOCOM 2023**, ACSAC 2020-2021, WiSec 2023, ICCPS 2022, ACM AsiaCCS 2021, Escar USA 2020.

- Journal reviewer (selected): **IEEE Transactions on Information Forensics & Security (T-IFS)**, **IEEE Transactions on Dependable and Secure Computing (TDSC)**, **IEEE Transactions on Intelligent Transportation Systems (T-ITS)**, **IEEE Communications Magazine**, **IEEE Transactions on Mobile Computing (TMC)**, IEEE Security & Privacy Magazine, IEEE Transactions on Cyber-Physical Systems (T-CPS), ACM Transactions on Privacy and Security (TOPS), Journal of Computer Security, IEEE Transactions on Network and Service Management (TNSM), MDPI Sensors.

- Organizer: 2022 NSF SaTC PI Meeting Break-Out Session "Cyber-Physical Security and Privacy" (***co-lead***).
- Publicity Chair: ACM CCS 2022.
- Society Committee Member: IEEE Emerging Transportation Technology Testing (ET3) Technical Committee (TC) 2023-now.

OTHER SERVICE/OUTREACH ACTIVITIES

- Panelist: NSF Panel (2019, 2020).
- Panelist: Yau High School Sciences Award in Computer Science, US Division (2019–2020).
- Faculty Advisor: Cyber@UCI (undergraduate cybersecurity club, 2019 – now)
  - Award: **5th place nationwide** at National CCDC (2021, *top 5 of 168+ university/college teams nationwide*)
  - Award: **1st place (Gold Medal)** at CCDC Western Regional (2021, *advaned to National CCDC **for the first time***
    - News Coverage: UCI's Cybersecurity Club Makes History, *Irvine Standard (local news paper)*, 06/10/2021.
  - Award: 2nd place (Silver Medal) at CCDC Western Regional (2022)
  - Award: 3rd place (Bronze Medal) at CCDC Western Regional (2020).