Qi Alfred Chen

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

Office: 3204 Bren Hall, 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 research projects towards systematically securing emerging autonomous systems and IoT such as autonomous driving systems, intelligent transportation systems, and smart home systems.

- *Sept. 2012 - Aug. 2018* **Research Assistant, RobustNet Research Group**, University of Michigan, Ann Arbor
  Advisor: Professor Z. Morley Mao (University of Michigan)
  – Formulated a general UI state inference attack based on a newly-discovered side channel, and built several new Android attacks (e.g., UI state hijacking) that demonstrated serious security implications.
  – Designed and implemented a static program analysis tool, PacketGuardian, to automatically detect off-path packet injection vulnerabilities in critical network protocols such as TCP and RTP.
  – Performed the first systematic analysis of a newly-exposed vulnerability, client-side name collision vulnerability, in internal network services due to the escalated name collision problem in the new gTLD era.
  – Performed the first security analysis of the emerging Connected Vehicle (CV) based traffic signal control system, and discovered several new vulnerabilities at the intelligent traffic control algorithm level.
  – Awarded the prestigious *Rackham Predoctoral Fellowship*, nominated for Microsoft Research PhD Fellowship

- *May 2015 - Oct. 2015* **Research Intern**, Verisign Labs, Reston
  Mentor: Eric Osterweil (Principal Scientist, Verisign Labs), and Matthew Thomas (Data Architect, Verisign Labs)
  – Identified a newly-exposed MitM attack vector by the name collision problem in new gTLD era, performed the first systematic study of the underlying problem causes and the vulnerability status in the wild.

PUBLICATIONS

Summary

Total Citations: **1065**, H-Index: **16**, i10-Index: **20** (Google Scholar, as of June 2020)

13 in top-tier security conferences (IEEE Security & Privacy, USENIX Security, ACM CCS, and ISOC NDSS)

7 in top-tier networking/mobile/systems conferences (ACM IMC, ACM MobiSys, ACM MobiCom, EuroSys)

4 in top-tier transportation/automobile conferences/journals (TRB/TRR, IEEE IV)

1 in top-tier software engineering conferences (ICSE)

1 in top-tier machine learning conferences (ICLR)

Conference/Workshop Publications

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

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 16.3%=158/972)*

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 16.3%=158/972)*

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 16.3%=158/972)*

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, 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 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, 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, 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, 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. Morle (top-tier conferences are highlighted in **bold**)y 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**)

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)*

Technical Reports

TR1. Earlence Fernandes, **Qi Alfred Chen**, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash, TIVOs: Trusted Visual I/O Paths for Android, University of Michigan Technical Report CSE-TR-586-14, August 2014.

PATENTS

P2. Eric M. Osterweil, Daniel R. McPherson, Matthew A. Thomas, **Qi Alfred Chen**, Detecting and Remediating Highly Vulnerable Domain Names Using Passive DNS Measurements, Publication Number US 20170279846 A1.

P1. Jie Hui, **Qi Chen**, Haokun Luo, Kevin Lau, Karthik Iyer, Kranthi Sontineni, Quality of Experience Diagnosis and Analysis in Wireless Communications, Publication Number US 20150326455 A1.

RESEARCH IMPACT

Selected Media Coverage

- 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

- US-CERT Alert TA16-144A: WPAD Name Collision Vulnerability
- CVE-2016-3898: Privilege escalation vulnerability in Android Telephony service
- CVE-2016-5227: Device authentication hijacking vulnerability in AirDroid
- AndroidID-21669196: Privilege escalation vulnerability in Android Short Message Service (SMS) service
- AndroidID-22541289: Privilege escalation vulnerability in Android Network Service Discovery (NSD) service
- AndroidID-23782371: Privilege escalation vulnerability in Android Telephony and Telecomm service

Selected Industry Discussions & Responses

- Email acknowledgements from Apple, Microsoft and Comcast on the reported client-side name collision vulnerabilities
- RIPE 72 discussion, 05/23/2016: *Alert (TA16144A) WPAD Name Collision Vulnerability*
- Verisign's remediation suggestions: *White Paper: Enterprise Remediation for WPAD Name Collision Vulnerability*

AWARDS AND HONORS

- 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)
- Rackham-CRLT Preparing Future Faculty (PFF) certificate, Rackham School, University of Michigan (2017)
- Internet of Things (IoT) Technology Research Award, Google (2016)
- 3rd place in Annual Code Optimization Contest, CSE dept., University of Michigan (2012)
- Graduate Fellowship, CSE dept., University of Michigan (2012)
- Top 100 Excellent Undergraduate Students of the Year, China Computer Federation (2012, *top 100 in China*)
- Outstanding Bachelor's Degree Thesis in Jiangsu province (2013, *top 0.1% in univ*)
- Model Outstanding Student, Nanjing University (2011, *top 0.3% in univ.*)
- National Scholarship, Ministry of Education of China (2010, *top 1.5% in univ.*)
- 1st prize in National Olympiad in Informatics in Provinces (NOIP), Ministry of Education of China (2007, *awarded the exemption of national college entrance exam*)

FUNDING

Total: $1,952,882, My share: $864,584:

- 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**.
- UCI ICS Research Award, "Towards Robust and Secure Autonomy Software," Total: $75,000 (2020-2021). Role: Lead PI. **My share: $37,500**.
- UCI ICS Research Award, "Exploring New Security Horizons for Emerging Autonomous Systems," Total: $75,000 (2019-2020). Role: Co-PI. **My share: $25,000**.
- UCI Academic Senate Council on Research, Computing, and Libraries (CORCL), "Attack Surface Analysis for Cybersecurity Research in Emerging Autonomous Vehicle Systems," Total: $2,885 (2019). Role: Single PI. **My share: $2,885**.

TEACHING & MENTORING EXPERIENCE

- Instructor, CS 134 Computer and Network Security, UC Irvine, Fall 2019
  – Undergraduate-level course on foundational work and current topics in elements of cryptography and network security.

- Instructor, CS 295 Advanced Computer and Network Security, UC Irvine, Spring 2019
  – Graduate-level course on foundational work and current topics in computer and network security.

- 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.
  – Course evaluator, 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.*"

- Research advising and mentoring (**Total: 4 Ph.D., 3 M.S., 24 B.S.**)
  – Junjie Shen (UCI Ph.D., 2018/7–, **NDSS'19 Distinguished Poster Presentation Award**, **NDSS'20 Best Technical Poster Award**): Autonomous CPS software security. *Publications: Usenix Security'20 (1st author), ICSE'20, ICLR'20.*
  – Takami Sato (UCI M.S., 2018/10–2019/9, UCI Ph.D., 2019/9–, **NDSS'20 Best Technical Poster Award**): Machine learning security in autonomous CPS.
  – Ningfei Wang (UCI Ph.D., 2019/9–, **NDSS'20 Best Technical Poster Award**): Autonomous CPS software security.
  – Ziwen Wan (UCI Ph.D., 2019/9–): Autonomous CPS software security.
  – Jun Yeon Won (UCI M.S., 2018/07–2019/07, now OSU Ph.D., **NDSS'19 Distinguished Poster Presentation Award**): Autonomous CPS software security. *Publications: Usenix Security'20.*
  – Yulong Cao (UMich B.S., now UMich Ph.D.): Name collision problem, machine learning security. *Publications: ACM CCS'19 (1st author), Usenix Security'20, ACM CCS'17.*
  – Yucheng Yin (UMich B.S., now CMU Ph.D., **CRA Outstanding Undergraduate Researcher Award nominee**): Intelligent traffic control system security. *Publications: ISOC NDSS'18.*
  – Shiqi Wang (SJTU B.S., now Columbia Ph.D.): Smart home IoT platform security. *Publications: ISOC NDSS'17.*
  – *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 multidisciplinary design program* (UMich, Winter 2016, student mentor): Yidan Zhang, Chia-Yen Lee, Jinting Hayter, Lihui Qin, Abigail Grobbel.
  – *Other advised students*: Jong Ho Lee (UCI M.S., 2018/10–2019/09), Newman Cheng (UCI B.S., 2018/10–2020/07, now Columbia M.S.), Kyle Bartz (UCI B.S., 2018/09–2019/07, now in Amazon), Zeyuan Chen (UCI B.S., 2019/09–2020/07, now CMU M.S.), Kanglan Tang (UCI B.S., 2019/12–), Huilai Liu (UCI B.S., 2020/01–), Haonan Xu (UCI B.S., 2020/02–), Liangze Yu (UCI B.S., 2019/01–2019/07), Chen Wang (UCI B.S., 2019/10–2019/12), Artur Gharibkhanyan (UCI B.S., 2019/09–2019/11), Vincent Tran (UCI B.S., 2019/8–2019/9), Deepak Kumar (UMich B.S., now UIUC Ph.D.), Lei Ruan (Tsinghua B.S., now CWRU M.S.).

TALKS

- 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

- QoE Doctor: Diagnosing Mobile App QoE with Automated UI Control and Cross-layer Analysis
  – 11/05/2014: 14th ACM SIGCOMM Internet Measurement Conference (IMC'14), Vancouver

- 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

- PC chair: ACM AutoSec 2019-2020 (**co-founder**).
- PC member: Usenix Security 2021, ACSAC 2020, ACM AsiaCCS 2021, ACM AutoSec 2019-2020, Escar USA 2020, CPSIoTSec 2020, IEEE IoT S&P 2019, AdvMLCV 2019, SPML 2019, IEEE S&P Student PC 2017.
- Journal reviewer: 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 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.
- External reviewer/subreviewer: ACM CCS 2014, USENIX WOOT 2016.

UNIVERSITY SERVICES

- Member of Ph.D. Defense Committee:
  – 05/26/2020: Alexios Voulimeneas, UC Irvine, advised by Prof. Michael Franz
  – 03/18/2019: Yuru Shao, University of Michigan, advised by Prof. Z. Morley Mao
  – 05/15/2019: David Ke Hong, University of Michigan, advised by Prof. Z. Morley Mao

- Chair of Ph.D. Candidacy Examination Committee:
  – 11/27/2019: Junjie Shen, UC Irvine, other committee member: Prof. Gene Tsudik, Prof. Marco Levorato, Prof. Ardalan Amiri Sani, Prof. Josh Garcia

- Member of Ph.D. Candidacy Examination Committee:
  – 11/29/2018: Tatiana Bradley, UC Irvine, advised by Prof. Stanislaw Jarecki
  – 05/28/2019: Dokyung Song, UC Irvine, advised by Prof. Michael Franz
  – 06/03/2019: Seyed Mohammadjavad Seyed Talebi, UC Irvine, advised by Prof. Ardalan Amiri Sani
  – 06/03/2019: Yingtong Liu, UC Irvine, advised by Prof. Ardalan Amiri Sani
  – 06/06/2019: Ercan Ozturk, UC Irvine, advised by Prof. Gene Tsudik
  – 10/17/2019: Sumaya Almanee, UC Irvine, advised by Prof. Josh Garcia
  – 11/08/2019: Zahraa Marafie, UC Irvine, advised by Prof. Kwei-Jay Lin
  – 12/04/2019: Yoshimichi Nakatsuka, UC Irvine, advised by Prof. Gene Tsudik
  – 12/16/2019: Yuheng Cao, UC Irvine, advised by Prof. Kwei-Jay Lin

- Member of UCI CS Graduate Admissions Committee (2019-2020).

- Organizer of UCI CS Grad Visit Day (2019).

OTHER SERVICE/OUTREACH ACTIVITIES

- Panelist: NSF Panel (2019).

- Panelist: Yau High School Sciences Award in Computer Science, USA Division (2019).

- Faculty Advisor: Cyber@UCI (Cybersecurity Club in UCI, 2019 – now).