Qi Alfred Chen

Ph.D. Candidate, EECS, University of Michigan, Ann Arbor
Email: alfchen@umich.edu
Tel: 734-834-2916
Homepage: https://web.eecs.umich.edu/~alfchen/

RESEARCH INTEREST

Network security, systems security, software security, smartphone system security, IoT/CPS systems security, security vulnerability discovery and analysis

I am interested in network and systems security in general. The major theme of my research is to address security challenges through systematic problem analysis and mitigation leveraging rigorous techniques such as static/dynamic program analysis, software testing, and network measurement.

My research has developed this approach to systematically analyze, detect, and fix vulnerabilities in traffic signal control systems, smartphone OSes, network protocols, DNS, GUI systems, and access control systems. My current focuses are security problems in **smart systems and IoT**, e.g., smart home, smart transportation, and autonomous vehicle systems.

EDUCATION

- **Ph.D. in Computer Science and Engineering**, University of Michigan, Ann Arbor — Apr. 2018 (expected)
  – *Dissertation*: "Securing Smart, Connected Systems Through Systematic Vulnerability Analysis and Mitigation"
  – *Advisor* : Professor Z. Morley Mao
- **M.S. in Computer Science and Engineering**, University of Michigan, Ann Arbor — May. 2014
- **B.S. in Department of Computer Science and Technology**, Nanjing University, Nanjing, China — Jun. 2012

PUBLICATIONS

Summary

7 (*5 first-authors*) in top-tier security conferences (IEEE Security & Privacy, USENIX Security, ACM CCS, and ISOC NDSS)

4 (*1 first-authors*) in top-tier networking conferences (ACM IMC, ACM MobiCom)

2 in top-tier transportation/automobile conferences (TRB, IEEE IV)

Top-Tier Conference Publications

1. **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, To appear in the 25th Network and Distributed System Security Symposium (**NDSS'18**), San Diego, February 2018. *(acceptance rate 21.5%)*

2. **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, Proceedings of the 24th ACM Conference on Computer and Communications Security (**CCS'17**), Dallas, October 2017. *(acceptance rate 18.1%)*

3. **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, Proceedings of the 37th IEEE Symposium on Security and Privacy (**S&P'16**), San Jose, May 2016. *(acceptance rate 13.3%)*

4. **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, Proceedings of the 22nd ACM Conference on Computer and Communications Security (**CCS'15**), Denver, October 2015. *(acceptance rate 19.8%)*

5. **Qi Alfred Chen**, Zhiyun Qian, and Z. Morley Mao, Peeking into Your App without Actually Seeing It: UI State Inference and Novel Android Attacks, Proceedings of the 23rd USENIX Security Symposium (**USENIX Security'14**), San Diego, August 2014. *(acceptance rate 19.0%)*

6. **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, Proceedings of the 14th ACM SIGCOMM Internet Measurement Conference (**IMC'14**), Vancouver, November 2014. *(acceptance rate 22.9%)*

7. 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, To appear in the Transportation Research Board 2018 Annual Meeting (**TRB'18**), Washington, D.C., January 2018. *(selected for journal publication with acceptance rate 20.0%)*

8. Yunhan Jack Jia, Ding Zhao, **Qi Alfred Chen**, Z. Morley Mao, Towards Secure and Safe Appified Automated Vehicles, Proceedings of the 28th IEEE Intelligent Vehicles Symposium (**IV'17**), Redondo Beach, 2017. *(selected for oral presentation with acceptance rate 10.0%)*

9. 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, Proceedings of the 24th Network and Distributed System Security Symposium (**NDSS'17**), San Diego, February 2017. *(acceptance rate 16.0%)*

10. Yihua Guo, Feng Qian, **Qi Alfred Chen**, Z. Morley Mao, and Subhabrata Sen, Understanding On-device Bufferbloat for Cellular Upload, Proceedings of the 16th ACM SIGCOMM Internet Measurement Conference (**IMC'16**), Santa Monica, November 2016. *(acceptance rate 25.3%)*

11. Yuru Shao, Jason Ott, **Qi Alfred Chen**, Zhiyun Qian, and Z. Morley Mao, Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework, Proceedings of the 23rd Network and Distributed System Security Symposium (**NDSS'16**), San Diego, February 2016. *(acceptance rate 15.4%)*

12. 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, Proceedings of the 21th ACM Annual International Conference on Mobile Computing and Networking (**MobiCom'15**), Paris, France, September 2015. *(acceptance rate 18.4%)*

13. 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, Proceedings of the 20th ACM Annual International Conference on Mobile Computing and Networking (**MobiCom'14**), Maui, September 2014. *(acceptance rate 16.4%)*

Other Peer-Reviewed Publications

1. 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, Proceedings of the 2nd IEEE European Symposium on Security and Privacy (**Euro S&P'17**), Paris, France, April 2017. *(acceptance rate 19.6%)*

2. 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, Proceedings of the 20th International Conference on Financial Cryptography and Data Security (**FC'16**), Barbados, February 2016. *(acceptance rate 26.0%)*

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

4. Yu Stephanie Sun, Lei Xie, **Qi Alfred Chen**, Sanglu Lu, and Daoxu Chen, Efficient Route Guidance in Vehicular Wireless Networks, Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'14), Istanbul, Turkey, April 2014.

5. 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)*

6. **Qi Chen**, Wenmin Lin, Shui Yu, and Wanchun Dou, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, Proceedings of the 9th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC'11), Sydney, Australia, December 2011.

PATENTS

- 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.

- 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*

PROPOSAL WRITING

Research funding proposals I helped draft:

- Mcity (University of Michigan), "Cybersecurity of Transportation Infrastructure in a Connected Vehicle Environment," ***Awarded*, $300,000. 1/1/2017 – 12/31/2018**, Co-PIs: Z. Morley Mao, Henry X. Liu.
- Mcity (University of Michigan), "Defense Strategies for Connected Transportation Infrastructure Under Cyber-attacks," ***Awarded*, $300,000. 1/1/2018 – 12/31/2019**. Co-PIs: Z. Morley Mao, Yiheng Feng.
- NSF Secure and Trustworthy Cyberspace (SaTC), "SaTC:CORE:Medium:Security Analysis for Next-generation Connected Vehicle based Transportation: New Attacks and Novel Defense Strategies," *Under review*. PI: Z. Morley Mao, Co-PI: Henry X. Liu.
- NSF Secure and Trustworthy Cyberspace (SaTC), "SaTC:CORE:Small: Securing Autonomous Vehicle Platform through Systematic Code Auditing and Dynamic Testing tackling Adversarial Machine Learning Threat Models," *Under review*. PI: Z. Morley Mao, Co-PI: Ding Zhao.
- Office of Naval Research (ONR), "Security Assurance through Protocol Customization: Novel Program Analysis and Machine Learning based Automation," *Under review*. PI: Z. Morley Mao, Co-PI: Scott Mahlke.

AWARDS AND HONORS

- 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 Bachelors 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*)

RESEARCH EXPERIENCE

- *Sept. 2012 - Now* **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.

TEACHING & MENTORING EXPERIENCE

- Instructor, Osher Lifelong Learning Institute (OLLI), Fall 2017, Winter/Spring 2018
  – 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.*"

- Guest lecturer, EECS 589 Advanced Computer Networks, Fall 2015
  – *Instructor*: Professor Z. Morley Mao
  – Guest lectures on research paper discussions, and special topics on domain name system (DNS) security.

- Student mentor, College of Engineering Multidisciplinary Design Program (MDP), Winter 2016
  – *Faculty mentor*: Professor Z. Morley Mao
  – *Team member*: Yidan Zhang, Chia-Yen Lee, Jinting Hayter, Lihui Qin, Abigail Grobbel
  – Guided team member in the design and implementation of a security vulnerability scanner for open source code.

- Research advising and mentoring
  – Yulong Cao (UMich B.S., now UMich Ph.D.): Contributed to the vulnerability analysis and exploit construction of name collision attacks on internal network service clients. *We co-authored the ACM CCS'17 paper.*
  – Yucheng Yin (UMich B.S., now applying Ph.D., *CRA Outstanding Undergraduate Researcher Award nominee*): Contributed to the security analysis and exploit construction of congestion and personal gain attacks on the intelligent traffic control system. *We co-authored the ISOC NDSS'18 paper.*
  – Shiqi Wang (SJTU B.S., now Columbia Ph.D.): Contributed to the development of the malware dataset for smart home IoT systems such as Samsung SmartThings. *We co-authored the ISOC NDSS'17 paper.*
  – Deepak Kumar (Umich B.S.,now UIUC Ph.D.): Investigated the usage of mDNS in popular local network applications, analyzed the potential security problems, and constructed proof-of-concept attacks.
  – Lei Ruan (Tsinghua B.S., now applying M.S.): Designed and implemented a scalable Android application crawler with the goal of building an Android application database that supports programmable code pattern search.

TALKS

- 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, ACM CCS FEAST workshop, 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 member: IEEE S&P Student PC 2017.
- Journal reviewer: IEEE Transactions on Information Forensics & Security (T-IFS), IEEE Transactions on Mobile Computing (TMC), IEEE Transactions on Network and Service Management (TNSM).
- External reviewer/subreviewer: ACM CCS 2014, USENIX WOOT 2016.