Yuan Tian

Room 422, Rice Hall
University of Virginia
Charlottesville, CA 22903

yuant@virginia.edu
650-862-0576
http://yuantiancmu.com

RESEARCH INTEREST

My research focuses on developing novel technologies for the security, privacy, and safety of CPS and mobile systems. I analyze and model the CPS system, drawing on program analysis, protocol analysis, machine learning, and human factors to understand the risks and develop systems that are secure and privacy preserving. My work has been published in top-tier security conferences (such as Oakland, CCS, Usenix Security and NDSS), and my work has generated real-world impact as countermeasures and design changes directly resulting from my research have been integrated into platforms (such as Android, Chrome, SmartThings, and iOS).

EDUCATION

2012 –2017 **Carnegie Mellon University (CMU)**
Department of Electrical and Computer Engineering
Ph.D student in Computer Security

2009 – 2012 **Beijing University of Posts and Telecommunications (BUPT)**
Department of Computer Science and Engineering
MSc in Information Security
GPA: 3.80/4 87/100 Ranking: 2/120

2005 – 2009 **Zhengzhou University (ZZU)**
Department of Information Engineering
BSc in Communication Engineering
GPA: 3.84/4 91/100 Major GPA: 3.94/4 Ranking: 1/160

EMPLOYMENT HISTORY

Assistant professor, **2017.9-Now**
Computer Science
University of Virginia

Research assistant, **2012.9-2017.8**
MEWS (Mobile, Embedded, & Wireless Security Lab), Cylab,
Department of Electrical and Computer Engineering,
Carnegie Mellon University

Security Intern, **2015.11-2016.2**
Security Infrastructure team, Facebook

Research Intern, **2015.5-2015.8**
System research group, Microsoft Research

Teaching Assistant, **2013.9-2015.12**
Courses: Mobile security, Web security and performance
Department of Electrical and Computer Engineering, Information Networking Institute
Carnegie Mellon University

Research Intern, **2013.5-2013.8**
Security group, Samsung

Research assistant, **2012.1-2012.6**
NISL (Network and Information Security Lab),
Tsinghua University

Research assistant, **2009.9-2011.12**
State Key Laboratories of Networking and Switching Technology,
Beijing University of Posts and Telecommunications

Teaching Assistant, **2010.9-2011.6**
Courses: Computer Networks, Signal Processing
Computer Science Department,
Beijing University of Posts and Telecommunications

PUBLICATIONS

1. Y. Zhuang, A. Rafetseder, Y. Hu, **Y. Tian**, J. Cappos, "Sensibility Testbed: Automated IRB Policy Enforcement in Mobile Research Apps", *to appear in HotMobile*, 2018, Acceptance rate: 29.2%
2. F. Suya, **Y. Tian**, D. Evans, P. Papotti, "Query-limited Black-box Attacks to Classifiers", *NIPS workshop on machine learning and computer security*, 2017
3. **Y. Tian**, N. Zhang, Y. Lin, X. Wang, X. Guo, P. Tague, "SmartAuth: User-Centered Authorization for the Internet of Things", *26th Usenix Security Symposium (Usenix Security), 2017*. Acceptance rate: 16.3%
4. A. Alanwar, B. Balaji, **Y. Tian**, S. Yang and M. Srivastava, "EchoSafe: Sonar-based Verifiable Interaction with Intelligent Digital Agents", *1st ACM Workshop on the Internet of Safe Things (SafeThings)*, co-located with Sensys, 2017
5. P. Marinescu, C. Parry, M. Pomarole, **Y. Tian**, P. Tague, I. Papagiannis, "IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks ", 38th IEEE Symposium on Security and Privacy (Oakland), 2017. Acceptance rate: 13.3%, Facebook news
6. **Y. Tian**, P. Tauge, "IoT security challenges", *HotSec,* 2017
7. **Y. Tian**, S. Chen, E. Chen, X. Ma, X. Wang, and P. Tague, "Swords and Shields - A Study of Mobile Game Hacks and Existing Defenses", *2016 Annual Computer Security Applications Conference (ACSAC)*, 2016. Acceptance rate: 22.8%, CMU headline
8. **Y. Tian**, Y. Pei, E. Chen, S. chen, R. Kotcher, and P. Tauge, "1000 Ways to Die in Moble OAuth", *Black Hat*, 2016. Top 10 Must-See Blackhat Talks
9. L. Bauer, S. Cai, L. jia, T. Passaro, M. Stroucken, and **Y. Tian**, "Run-time Monitoring and Formal Analysis of Information Flows in Chromium", *Network and Distributed System Security Symposium (NDSS)*, 2015. Acceptance rate: 16.9%
10. **Y. Tian**, B. Liu, W. Dai, B. Ur, P. Tague, and L. Cranor, "Supporting Privacy-Conscious App Update Decisions with User Reviews", *to appear in ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM),* 2015. Acceptance rate: 38%
11. H. Wang, A. Moshchuk, M. Gamon, M. Haraty, S. Iqbal, E. Brown, A. Kapoor, C. Meek, E. Chen, **Y. Tian**, J. Teevan, M. Czerwinski, and S. Dumais, "The Activity Platform", *Workshop on Hot Topics in Operating Systems(HotOS),* 2015. Acceptance rate: 31.8%
12. E. Chen, S. Chen, Y. Pei, **Y. Tian**, R. Kotcher, and P. Tague, "OAuth Demystified for Mobile Application Developers", *ACM Conference on Computer and Communications Security (CCS)*, 2014. Acceptance rate: 18.6%
13. L. Bauer, S. Cai, L. Jia, T. Passaro and **Y. Tian,** "Analyzing the Dangers Posed by Chrome

Extensions: A Case for Information-Flow-Based Protection", *IEEE Conference on Communications and Network Security(CNS),* 2014. Acceptance rate: 29.2%

14. Y. Kim, **Y. Tian**, L. Nguyen and P. Tague, "LAPWiN: Location-Aided Probing for Protecting User Privacy in Wi-Fi Networks", *IEEE Conference on Communications and Network Security(CNS),* 2014. Acceptance rate: 29.2%

15. **Y. Tian**, K. Liu, A. Bhosale, L. Huang, P. Tague, and C. Jackson, "All Your Screens Are Belong to Us: Attacks Exploiting the HTML5 Screen Sharing", *35th IEEE Symposium on Security and Privacy (Oakland 2014)*, 2014. Acceptance rate: 13.1%

16. S. Kywe, C. Landis, Y. Pei, J. Satterfield, **Y. Tian**, and Patrick Tague, "PrivateDroid: Private Browsing Mode for Android", *IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2014*

17. L. Nguyen, **Y. Tian**, S. Cho, W. Kwak, S. Parab, Y. Kim, P. Tague, and J. Zhang, "UnLocIn: Unauthorized Location Inference on Smartphones without Being Caught", *International Conference on Security and Privacy in Mobile Information and Communication Systems (PRISMS)*, June 2013.

18. **Y.Tian**, C. Zheng, A. Desnos, "APKInspector: Static Analysis of Android Applications", *Honeynet Workshop, 2013*

- **Posters**

19. **Y. Tian**, E. Chen, J. Sousa, P. Tague, and H. Wang, "Privacy-Preserving Context Sharing in Social Platforms", *25th Usenix Security Symposium (Usenix Security), 2016*

20. **Y. Tian**, K. Liu, A. Bhosale, L. Huang, P. Tague, and C. Jackson, "Attacks Exploiting the HTML5 Screen Sharing", *Women in Cyber Security (WiCys), 2014*

21. Y. Kim**, Y. Tian**, L. Nguyen, and P. Tague, "LAPWiN: Location-Aided Probing in Wi-Fi Networks" ,*34th IEEE Symposium on Security and Privacy (Oakland 2013)*, 2013

22. A. Athreya, Y. Kim, X. Wang, **Y. Tian**, and P. Tague, "Packet Conductance for Statistical Intrusion Detection in Anonymous Networks", *34th IEEE Symposium on Security and Privacy (Oakland 2013)*, 2013

- **Patents**

23. Y. Kim**,** L. Nguyen, **Y. Tian**, and P. Tague, "LAPWiN: Location-Aided Probing in Wi-Fi Networks", pending

- **Technical Reports**

24. **Y. Tian**, C. Herley, and S. Schechter, "Exploring Mechanisms to Defend Against Online Password Guessing", Microsoft Technical Report, 2016, News

25. L. Bauer, S. Cai, L. jia, T. Passaro, M. Stroucken, and **Y. Tian**, "Run-time Monitoring and Formal Analysis of Information Flows in Chromium", CMU Cylab Technical Report, 2015

TALKS

- SmartAuth, *Usenix Security' 17,* Vancouver, Canada
- IoT security challenges, *HotSec' 17*, Vancouver, Canada
- Adversial machine learning, Alibaba Machine Learning Forum, Seattle, WA, 2017
- Protecting User Security and Privacy in Modern and Emerging Platforms, Rising Star in EECS, Pittsburgh, PA, 2016
- Introduction to Android Security, Cal Poly, San Luis Obispo, CA, 2016

- Mobile OAuth: attacks and defenses, Baidu, Sunnyvale, CA, 2016
- 1000 Ways to Die in Mobile OAuth, *Blackhat'16*, Las Vegas, NV, 2016
- Privacy-Preserving Context Sharing for Social Platforms, *Usenix Security' 16*, poster session, Austin, TX, 2016
- Invariant Detector: Automatically Protecting User Privacy in Graph-Based Web Applications, Facebook, London, UK, 2016
- Supporting Privacy-Conscious App Update Decisions with User Reviews*, SPSM'15*, Denver, CO, 2015
- Use Guessed Passwords to Stop Online Password Guessing Attacks, Microsoft Research, Redmond, WA, 2015
- Analyzing the dangers posed by Chrome extensions, *CNS'14*, San Francisco, CA, 2014
- Attacks Exploiting the HTML5 Screen Sharing", *WiCys'14,* Nashville, TN *2014*
- Privacy Preserving Large-Scale Machine Learning, Qualcomm, 2014
- All Your Screens Are Belong to Us: Attacks Exploiting the HTML5 Screen Sharing API, *Oakland'14*, 2014
- APKInspector: Static Analysis for Android, *Honeynet 2013*, Dubai, UAE, 2013

AWARDS & HONORS

- 2016 Invited to Rising Star in EECS Workshop (69 female researchers across the world)
- 2015 BlackHat future female leaders
- 2014 Microsoft Research Fellowship Final list
- 2014 Qualcomm Innovation Fellowship Final list
- 2014 Best poster runner up at Women in Cyber Security Conference
- 2014 Security Hall of Fame for Facebook, Dropbox, Evernote, and Tencent
- 2014 CCS Student Travel Grant
- 2014 Oakland Student Travel Grant
- 2013 Two API prizes in AngelHack Silicon Valley
- 2012 Dean's Fellowship, Carnegie Mellon University
- 2010 – 2011 IBM Chinese Excellent Student Fellowship- 74 students from 30 top universities
- 2009 – 2010 CHANGFEI Scholarship of China - 1 out of 300 CS master students in BUPT
- 2008 China Soong Ching Ling Female Student Fellowship

PROFFESIONAL SERVICES

Workshop co-chair:

- TPC co-chair for ACM Workshop on the Internet of Safe Thing, 2017

TPC member:

- Usenix Security 2018
- Radical and Experimental Security Workshop 2018

Reviewers:

- IEEE Pervasive Computing 2017
- Transactions on Dependable and Secure Computing 2017
- Journal of Security and Communication Networks 2016

- Ubicomp 2015
- ISWC 2015

External Reviewers:

CCS 2013-2014, 2016 NDSS 2014, 2017 Oakland 2014
ACSAC 2013- 2014 Infocom 2015,2017 CNS 2014-2016
Mobicom 2014 WCNC 2013-2016 SECON 2014
ASIACCS 2014-2015 WiSec 2014-2016

LEADERSHIP & ACTIVITIES

- 2015 NASA 75-year Anniversary Open House volunteer
- 2014-2015 CMU SV Graduate Student Organization Chair
- 2014 CNS student volunteer
- 2014 CMU Privacy Day volunteer