Yuan Tian

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

yuant@virginia.edu
650-862-0576
https://www.ytian.info/

RESEARCH INTEREST

My research focuses on developing novel technologies for the security, privacy of Cyber-Physical Systems (CPS) and machine learning systems. Drawing on program analysis, protocol analysis, machine learning, and human factors, I identify the risks and develop systems that are secure and privacy preserving.

EDUCATION

2012.9 –2017.8 **Carnegie Mellon University (CMU)**
Ph.D., Department of Electrical and Computer Engineering

2009.9 – 2012.3 **Beijing University of Posts and Telecommunications (BUPT)**
MSc, Department of Computer Science and Engineering

2005.9 – 2009.6 **Zhengzhou University (ZZU)**
BSc, Department of Information Engineering

APPOINTMENTS

Assistant professor, **2017.9-Now**
Computer Science, Linklab
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,
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

AWARDS & HONORS

- 2020 NSF CAREER Award
- 2019 CSAW Best Security Paper Award (3rd place)
- 2019 Amazon Research Award
- 2019 NSF CRII Award
- 2019 UVA Engineering Research Innovation Award
- 2018 UVA Engineering Research Innovation Award
- 2016 Rising Stars in EECS
- 2014 Microsoft Research Fellowship Final list
- 2014 Qualcomm Innovation Fellowship Final list
- 2014 Best poster runner up at Women in Cyber Security Conference
- 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 Excellent Student Fellowship
- 2009 – 2010 CHANGFEI Scholarship of China - 1 out of 300 CS master students in BUPT
- 2008 China Soong Ching Ling Female Student Fellowship

PUBLICATIONS

Peer-Reviewed Conference and Journal Papers:

1. **[Ubicomp'21]** F. Shezan, H. Hu, J. Wang, G. Wang, and **Y. Tian**, "VerHealth: Vetting Medical Voice Applications through Policy Enforcement", to appear in the *Proceedings of The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp)*, 2021

2. **[AAAI'21]** S. Zawad, A. Ali, P. Chen, A. Anwar, Y. Zhou, N. Baracaldo, **Y. Tian**, F. Yan, "Curse or Redemption? How Data Heterogeneity Affects the Robustness of Federated Learning", to appear in the *Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI-21), 2021*

3. **[NeurIPS'20]** J. Chi*, H. Zhao*, **Y. Tian**, G. Gordon, "Trade-offs and Guarantees on Adversarial Representation Learning for Information Obfuscation", in *Thirty-fourth Conference on Neural Information Processing Systems (NeurIPS)*, Dec 2020. 12 pages, acceptance rate: 20%.

4. **[EMNLP Findings'20]** W. Ahmad*, J. Chi*, **Y. Tian**, K. Chang, "PolicyQA: A Reading Comprehension Dataset for Privacy Policies", in the *2020 Conference on Empirical Methods in Natural Language Processing* (*EMNLP Findings)*, Nov 2020.

5. **[USENIX Security'20]** F. Suya, J. Chi, D. Evans, and **Y. Tian**, "Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries", to appear in the *29th Usenix Security Symposium (Usenix Security), August 2020.* 18 pages, acceptance rate: ~17%

6. **[USENIX Security'20]** Z. Tang, K. Tang, M. Xue, **Y. Tian**, S. Chen, M. Ikram, T. Wang, H. Zhu, "iOS, Your OS, Everybody's OS: Vetting and Analyzing Network Services of iOS Apps", in the *29th Usenix Security Symposium (Usenix Security), August 2020.* 19 pages, acceptance rate: ~17%

7. **[Ubicomp'20]** Y. Lee, Y. Zhao, J. Zeng, K. Lee, N. Zhang, F. Shezan, **Y. Tian**, K. Chen, X. Wang, "SPEAKER-RADAR: a Sonar-based Liveness Detection System for Protecting Smart Speakers Against Remote Attackers", in the *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), September 2020*.

8. **[IEEE SP Magazine'20] Y. Tian**, C. Herley, S. Schechter, "StopGuessing: Using Guessed Passwords to Thwart Online Guessing", in *IEEE Security and Privacy Magazine,* invited paper, June 2020.

9. **[WWW'20]** F. Shezan, H. Hu, J. Wang, G. Wang, and **Y. Tian,** "Read Between the Lines: An Empirical Measurement of Sensitive Applications of Voice Personal Assistant Systems", in *the Web Conference (WWW)*, May 2020. 12 pages, acceptance rate: 19%.

10. **[VEHITS'20]** T. Le, I. Elsayed-Aly, W. Jin, S. Ryu, G. Verrier, T. Rahat, B. Park, **Y. Tian**, "Evaluating the Dedicated Short-range Communication for Connected Vehicles against Network Security Attacks", in *the 6th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS),* April 2020.

11. **[NDSS'20]** F. Shezan, K. Cheng, Z. Zhang, Y. Cao, **Y. Tian**, "TKPERM: Cross-platform Permission Knowledge Transfer to Detect Overprivileged Third-party Applications", in *the Network and Distributed System Security Symposium (NDSS), February 2020*. 15 pages, acceptance rate: ~18%

12. **[IEEE Design&Test'20]** J. Stankovic, H. Alemzadeh, B. Campbell, J. Lach, F. Lu, C. Fleming, J. Goodall, T. Odumosu, D. Quinn, **Y. Tian**, K. Tobler, "A Graduate Curriculum in Cyber Physical Systems", in *IEEE Design & Test*, 2020

13. **[ASE'19]** T. Rahat, Y. Feng, and **Y. Tian**, "OAuthLint: An Empirical Study on OAuth Bugs in Android Applications", to appear in the *34th IEEE/ACM International Conference on Automated Software Engineering (ASE), December 2019.* 12 pages, acceptance rate: 20%

14. **[Usenix Security'19]** D. Wang, P. Wang, D. He, and **Y. Tian**, "Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users", in the *28th Usenix Security Symposium (Usenix Security), August 2019.* 18 pages, acceptance rate: ~17%. **News**

15. **[EuroS&P'19] Y. Tian**, C. Herley, S. Schechter, "StopGuessing: Using Guessed Passwords to Thwart Online Guessing", in *IEEE European Symposium on Security and Privacy (EuroS&P),*

July 2019. 14 pages, acceptance rate: 20%. **Invited to IEEE Security and Privacy Magazine.** **News**

16. **[IEEE S&P'19]** N. Zhang, X. Mi, X. Feng, X. Wang, **Y. Tian**, F. Qian, "Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems", in the *40th IEEE Symposium on Security and Privacy (Oakland), May* 2019. 16 pages, acceptance rate: 12%. **CSAW Best Security Paper Award (3rd place). News**

17. **[IEEE S&P'19]** Y. Chen, M. Zha, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, F. Suya, **Y. Tian**, K. Chen, X. Wang, W. Zhou, "Demystifying Hidden Privacy Settings in Mobile Apps", in the *40th IEEE Symposium on Security and Privacy (Oakland),* May 2019. 17 pages, acceptance rate: 12%

18. **[USENIX Security'17] Y. Tian**, N. Zhang, Y. Lin, X. Wang, X. Guo, P. Tague, "SmartAuth: User-Centered Authorization for the Internet of Things", in the *26th Usenix Security Symposium (Usenix Security),* pp. 361-378, August 2017. 18 pages, acceptance rate: 16.3%

19. **[IEEE S&P'17]** P. Marinescu, C. Parry, M. Pomarole, **Y. Tian**, P. Tague, I. Papagiannis, "IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks ", the *38th IEEE Symposium on Security and Privacy (Oakland)*, pp. 1094-1109, May 2017. 16 pages, acceptance rate: 13.3%, **News**

20. **[ACSAC'16] 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 ACM Annual Computer Security Applications Conference (ACSAC)*, pp. 386-397, November 2016. 12 pages, acceptance rate: 22.8%, **News**

21. **[NDSS'15]** 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)*, February 2015. 15 pages, acceptance rate: 16.9%

22. **[CCS'14]** 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)*, pp. 892-903, November 2014. 12 pages, acceptance rate: 18.6%

23. **[TrustCom'14]** 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),* pp. 27-36, September 2014. 10 pages, acceptance rate: 18.3%.

24. **[CNS'14]** 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), pp. 184-192, June 2014. 9 pages, acceptance rate: 29.2%

25. **[CNS'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),* pp. 427-435, June 2014. 9 pages, acceptance rate: 29.2%

26. **[IEEE S&P'14] 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)*, pp. 34-48, May 2014. 15 pages, acceptance rate: 13.1%

27. **[PRISMS'13]** 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)*, pp. 1-8, June 2013. 8 pages, acceptance rate: NA

Peer-reviewed Workshop Papers

28. **[MLWG'19]** J. Chi, H. Zhao, **Y. Tian**, G. Gordon, "Privacy Guarantees for Adversarial Task-Specific Privacy Preservation", to appear in *NeurIPS 2019 Workshop on ML with Guarantees,* December 2019.

29. **[SafeThings'19]** S. Liu, Y. Wei, J. Chi, F. Shezan and **Y. Tian**, "Side Channel Attacks in GPU-Virtualization-Based Computation-Offload Systems", in *IEEE Workshop on the Internet of Safe Things (SafeThings),* co-located with Oakland 2019, May 2019. 6 pages, acceptance rate: 32%

30. **[WISECML'19]** Y. Yu, C. Li, M. Jonas, S. Shen, C. Ma, F. Shezan and **Y. Tian**, "Detecting Abnormal Behaviors in Smart Home", in *the Workshop on Machine Learning Security and Privacy: Experiences and Applications, co-located with MASS 2019,* November 2019.

31. **[ArchEdge'18]** J. Chi, E. Owusu, X. Yin, T. Yu, W. Chan, Y. Liu, S. Sim, H. Liu, J. Chen, V. Iyengar, P. Tague and **Y. Tian**, "Privacy Partition: A Privacy-preserving Framework for Deep Neural Networks in Edge Networks", in the *1st ACM/IEEE Workshop on Computing Architecture for Edge Computing (ArchEdge)*, October 2018

32. **[HotMobile'18]** Y. Zhuang, A. Rafetseder, Y. Hu, **Y. Tian**, J. Cappos, "Sensibility Testbed: Automated IRB Policy Enforcement in Mobile Research Apps", *in IEEE HotMobile*, February 2018, pp. 113-118, 2018. 6 pages, acceptance rate: 29.2%

33. **[MLSEC'17]** F. Suya, **Y. Tian**, D. Evans, P. Papotti, "Query-limited Black-box Attacks to Classifiers", *NIPS workshop on machine learning and computer security*, November 2017. 5 pages, acceptance rate: 40%

34. **[SafeThings'17]** A. Alanwar, B. Balaji, **Y. Tian**, S. Yang and M. Srivastava, "EchoSafe: Sonar-based Verifiable Interaction with Intelligent Digital Agents", the *1st ACM Workshop on the Internet of Safe Things (SafeThings)*, co-located with Sensys, pp. 38-43, November 2017. 6 pages, acceptance rate: 42%

35. **[SPSM'15] Y. Tian**, B. Liu, W. Dai, B. Ur, P. Tague, and L. Cranor, "Supporting Privacy-Conscious App Update Decisions with User Reviews", *ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM),* pp. 51-61*, November* 2015. 11 pages, acceptance rate: 38%

36. **[HotOS'15]** 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", *ACM Workshop on Hot Topics in Operating Systems (HotOS), May* 2015. 5 pages, acceptance rate: 31.8%

Posters

37. T. Le, I. ElSayed-Aly, W. Jin, S. Ryu, G. Verrier, T. Rahat, B. Park, and **Y. Tian**, "Poster: Attack the Dedicated Short-Range Communication for Connected Vehicles", in the 40th IEEE Symposium on Security and Privacy (Oakland), 2019.

38. G. Verrier, H. Chen, D. Evans, **Y. Tian**, "Poster: How is GDPR Affecting Privacy Policies? ", *the 27th USENIX Security Symposium (Usenix Security)*, August 2018.

39. F Suya, D Evans, **Y Tian**, "Poster: Adversaries Don't Care About Averages: Batch Attacks on Black-Box Classifiers ", *the 39th IEEE Symposium on Security and Privacy (Oakland*), May 2018

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

41. **Y. Tian**, K. Liu, A. Bhosale, L. Huang, P. Tague, and C. Jackson, "Attacks Exploiting the HTML5 Screen Sharing", *Women in Cyber Security (WiCys),* December 2014. **Best Poster Runner-Up.**

42. 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)*, May 2013.

43. 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)*, May 2013.

Patents

44. Y. Kim**,** L. Nguyen, **Y. Tian**, and P. Tague, "LAPWiN: Location-Aided Probing in Wi-Fi Networks", filed, May 2015

Technical Reports and Other Publications

45. G. Verrier, Y. Taylor, E. Fernandes, T. Kohno, **Y. Tian**, "SmartCity Security", *2018 USENIX Summit on Hot Topics in Security (HotSec)*, August 2018. 6 pages.

46. **Y. Tian**, P. Tauge, "IoT security challenges", in *USENIX Summit on Hot Topics in Security (HotSec), August* 2017. 2 pages.

47. **Y. Tian**, Y. Pei, E. Chen, S. chen, R. Kotcher, and P. Tauge, "1000 Ways to Die in Mobile OAuth", *Black Hat*, August 2016. News. 10 pages.

48. **Y. Tian**, C. Herley, and S. Schechter, "Exploring Mechanisms to Defend Against Online Password Guessing", Microsoft Technical Report, May 2016. 15 pages.

49. 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, February 2015. 20 pages.

50. **Y. Tian**, C. Zheng, A. Desnos, "APKInspector: Static Analysis of Android Applications", *Honeynet Workshop, February 2013*. 5 pages.

PROFESSIONAL ACTIVITIES

Conference and Workshop Organizers:

- **[IEEE S&P]** Shadow PC Chair for IEEE Symposium for Security and Privacy (Oakland) 2021
- **[SafeThings]** Co-chair for IEEE Workshop on the Internet of Safe Things 2019, 2021, co-located with IEEE Oakland
- **[WISECML]** Co-chair for Workshop on Machine Learning Security and Privacy: Experiences and Applications, co-located with MASS 2019
- **[USENIX Security]** Poster chair for Usenix Security 2018
- **[SafeThings]** TPC co-chair for ACM Workshop on the Internet of Safe Thing, co-located with ACM Sensys 2017

TPC members:

- **[USENIX Security]** Usenix Security 2018, 2020-2021
- **[IEEE S&P]** IEEE Oakland 2020-2021
- **[NDSS]** NDSS 2019-2021
- **[CCS]** ACM CCS 2018-2019
- **[EuroS&P]** IEEE EuroS&P 2020-2021
- **[AsiaCCS]** ACM AsiaCCS 2019-2020
- **[DAC]** Design Automation Conference (Embedded and Cross-Layer Security Track) 2021
- **[Sensys]** ACM Sensys 2020
- **[CSF]** ACM CSF 2020
- **[SecDev]** IEEE SecDev 2020
- **[AAAI]** AAAI 2019
- **[AutoSec]** ACM AutoSec Workshop 2019-2020
- **[SafeThings]** IEEE SafeThings Workshop 2020-2021
- **[AI4Mobile]** IEEE AI4Mobile Workshop 2019

Grant Panel Reviewers:

- **[NSF]** National Science Foundation (NSF) Review Panel (×3): 2020
- **[NSF]** National Science Foundation (NSF) Review Panel (×1): 2019
- **[NSF]** National Science Foundation (NSF) Review Panel (×1): 2019

Journal and Magazine Reviewers:

- **[TDSC]** IEEE Transactions on Dependable and Secure Computing 2017-2020
- **[TMC]** IEEE Transactions on Mobile Computing 2020
- **[HEALTH]** ACM Transactions on Computing for Healthcare 2020
- **[SP]** IEEE Security and Privacy 2019
- **[LES]** IEEE Embedded System Letters 2019
- **[Pervasive]** IEEE Pervasive Computing 2017

GRANTS

External Gants:

1. **CAREER: Secure Voice-Controlled Platforms** (Sole PI)
   U.S. National Science Foundation (NSF)
   Duration: 09/2020-08/2024
   Total Budget: $490,438.00
   My Share: $490,438.00

2. **CICI: RDP: Enforcing Security and Privacy Policies to Protect Research Data** (PI)
   Co-PI: Kai-Wei Chang (University of California, Los Angeles), Yanyan Zhuang (University of Colorado Colorado Springs), Byoung-Do Kim
   U.S. National Science Foundation (NSF)
   Duration: 09/2019-08/2022
   Total Budget: $924,503.00
   My Share: $416,320.00

3. **CRII: SaTC: Improving the Usability and Effectiveness of Security and Privacy Settings in Mobile Apps** (Sole PI)
   U.S. National Science Foundation (NSF)
   Duration: 06/2019--05/2021
   Total Budget: $174,977.00
   My Share: $174,977.00

4. **Dynamic Graph-based Anomaly Detection for Cloud Computing** (Sole PI)
   Amazon Research Award
   Duration: 06/2019-05/2020
   Total Budget: $74,000.00
   My Share: $74,000.00

5. **A Systematic Evaluation of Smart City Security and Privacy** (Co-PI, PI at UVa)
   Virginia State
   PI: Adwait Nadkarni (College of William & Mary)
   Duration: 12/2020-12/2021
   Total Budget: $194,850.00
   My Share: $99,390.00

6. **CDS&E: Collaborative Research: Private Data Analytics, Synthesis, and Sharing for Large-Scale Multi-Modal Smart City Mobility Research** (Co-PI, PI at UVa)
   U.S. National Science Foundation (NSF)
   Duration: 06/2020-06/2023

PI: Desheng Zhang (Rutgers University), Co-PI: Dimitris Metaxas (Rutgers University)
Total Budget: $516,000.00
My Share: $165.000

7. **Training in the Integration of Cyber Physical Systems and Security** (Co-PI)
   Virginia State
   PI: John Stankovic, Co-PI: Lu Feng
   Duration: 06/2020-06/2021
   Total Budget: $77,000.00
   My Share: $25,000.00

8. **NRT: A Graduate Traineeship in Cyber-Physical Systems** (Senior Personnel)
   U.S. National Science Foundation (NSF)
   PI: John Stankovic, Co-PI: John Lach, Jonathan Goodall, Homa Alemzadeh, Cody Fleming
   Senior Personnel: Lu Feng,
   Duration: 09/2018--08/2023
   Total Amount: $ 2,971,756.00
   My Share: $ 297,175.00

9. **CRI: II-NEW: The Living Link Lab: Infrastructure for Enhancing Occupant Experience and Building Operations** (Co-PI)
   PI: Arsalan Heydarian, Co-PI: Brad Campbell, Nicola Bezzo, Matt Gerber
   U.S. National Science Foundation (NSF)
   Duration: 08/2018-08/2021
   Total Budget: $ 980,000.00
   My Share: $ 190, 000.00

Internal Grants:

10. **Privacy-Preserving Machine Learning via Robust Learning and Noisy Computation** (Co-PI)
    SEAS Research Innovation Award
    PI: David Wu, Co-PI: David Evans, Mohammad Mahmoody
    Duration: 09/2019-06/2020
    Total Amount: $ 121, 911
    My Share: $30,497

11. **Foundations of Automated Risk Assessment for Cyber-Physical Systems** (Co-PI)
    SEAS Research Innovation Award
    PI: Cody Fleming, Co-PI: Madhur Behl
    Duration: 06/2018-06/2019
    Total Amount: $ 90,000
    My Share: $ 30,000

12. **Cyber-Attacks on Integrated Clinical Environments** (Co-PI)
    SEAS Research Innovation Award

PI: Homa Alemzadeh

Duration: 06/2018-06/2019

Total Amount: $ 60,000

My Share: $ 30,000

TALKS

- Enforcing Security and Privacy Policies to Protect Research Data, Invited Talk, NSF Trusted Cyber Infrastructure Seminar, 2020
- AI for Information Security: Challenges and Opportunities, Invited Talk, Amazon, 2020
- Mobile and IoT Security, Invited Talk, Girls Who Code, 2020
- Secure Voice-Controlled Platforms, Invited Talk, University of Chicago, Chicago, IL, 2019
- Create Cyber-Physical-System Classes for Future Researchers and Engineers, NSF NRT PI meeting, Chicago, IL, 2019
- Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users, *Usenix Security*, 2019
- IoT Security and Privacy, Invited Talk, Ford, Palo Alto, CA, 2019
- Smarthome Security and Privacy, Invited Talk, CMU SV, Moffett Field, CA, 2019
- StopGuessing: Using Guessed Passwords to Thwart Online Guessing", *EuroS&P,* Stockholm, Sweden, 2019
- Security and Privacy Protections in the Internet of Things, Invited Talk, *IEEE PAC 2018*, Washington DC, 2018
- Emerging Privacy Challenges Faced by Our Changing Society, Panelist, *IEEE HotPrivacy 2018,* Washington DC, 2018
- Security for self-driving cars, Invited Talk, Baidu, Sunnyvale, CA, 2018
- SmartAuth, *Usenix Security' 17,* Vancouver, Canada, 2017
- IoT security challenges, *HotSec' 17*, Vancouver, Canada, 2017
- Adversarial machine learning, Alibaba Machine Learning Forum, Invited Talk, Seattle, WA, 2017
- Mobile and IoT Security, Seminar, ECE UCLA, CA, 2017
- Protecting User Security and Privacy in Modern and Emerging Platforms, Rising Star in EECS, Pittsburgh, PA, 2016
- Introduction to Android Security, Invited Talk, Cal Poly, San Luis Obispo, CA, 2016
- Mobile OAuth: attacks and defenses, Invited Talk, 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

OUTREACH ACTIVITIES

- 2020 Faculty Consultant for Girls Who Code at UVa
- 2018 Judge for the Student Research Presentations
- 2018 Mentor for CyberSecurity Summer School for High School Teachers
- 2018 Faculty Advisor for the Computer and Network Security Club
- 2016 Women in ECE organizer
- 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

TEACHING

- CS6333 Mobile and IoT Security, Fall 2020
- CS 4630 System Security: Defense Against the Dark Arts, Spring 2020
- CS 8501 Hot Topics in Security and Privacy, Fall 2019
- CS 4630 System Security: Defense Against the Dark Arts, Spring 2019
- CS 6501 Mobile and IoT Security, Fall 2018
- CS 4630 System Security: Defense Against the Dark Arts, Spring 2018
- CS 6501 Mobile Security, Fall 2017

ADVISING

Ph.D. Students:

- Fnu Suya (co-advised with David Evans) 2017 - Now
- Faysal Hossain 2018 - Now (Linklab Outstanding Graduate Researcher)
- Jianfeng Chi 2018 - Now
- Tu Le 2018 -Now
- Tamjid Al Rahat 2018 -Now

Master Students:

- Kamya mehul Desai
- Weizhao Jin
- Kaiming Cheng
- Zoya Yeprem Gerdabad

Undergraduate Students:

- Akanksha Alok
- Amber Liu
- Elena Long
- Vanessa Barlow
- Ethan Gumabay
- Shaishav Naik
- Farid Rajabi Nia
- Chenghan Zhou (honorable mention for CRA Outstanding Undergraduate Researcher Award)
- Sophia Cheung
- Jordan Farquhar
- Niel Ketkar
- Alex Kwakye

Highschool Student:

- Stephen Newman