# Gang Wang

Associate Professor of Computer Science
University of Illinois at Urbana-Champaign (UIUC)

Thomas M. Siebel Center for Computer Science
201 North Goodwin Avenue, RM 4316
Urbana, IL 61801-2302
gangw@illinois.edu
Tel: 217-244-1008
https://gangw.cs.illinois.edu

## EDUCATION

**University of California, Santa Barbara**, Santa Barbara, CA. 2010 – 2016
Ph.D. in Computer Science
Advisors: Ben Y. Zhao, and Heather Zheng

**Tsinghua University**, Beijing, China. 2006 – 2010
Bachelor of Engineering, Electronic Engineering

## APPOINTMENTS

**University of Illinois at Urbana-Champaign**, Urbana, IL.
Associate Professor, Department of Computer Science Aug. 2023 – Present
Assistant Professor, Department of Computer Science Aug. 2019 – Aug. 2023
Affiliate Faculty, University of Illinois Coordinated Science Laboratory (CSL) Sep. 2023 – Present
Affiliate Faculty, Department of Electrical and Computer Engineering Nov. 2020 – Present
Affiliate Faculty, Informatics Programs, School of Information Sciences Sep. 2021 – Present

**Virginia Tech**, Blacksburg, VA.
Assistant Professor, Department of Computer Science Aug. 2016 – Aug. 2019

**Microsoft Research**, Redmond, WA.
Research Intern; with Jay Stokes, Weidong Cui, and Helen Wang Jun. 2014 – Sep. 2014

**LinkedIn,** Mountain View, CA.
Data Scientist Intern; with Vicente Silveira, and Karthik Ramasamy Jun. 2012 – Sep. 2012

**Microsoft Research**, Redmond, WA.
Research Intern; with Cormac Herley, and Jay Stokes Jun. 2011 – Sep. 2011

## RESEARCH INTERESTS

Security and Privacy; Data Mining; Internet Measurement; Human-Computer Interaction

## AWARDS

USENIX Security Noteworthy Reviewers, *USENIX Security* (2023)
MobiSys Excellent Service: as Student Travel Grants co-Chair, MobiSys (2023)
ACM CCS Best Reviewer Award, *ACM CCS* (2022)
Amazon Research Awards, *Amazon* (2021)
Teacher Ranked as Excellent/Outstanding by their Students, *UIUC* (2019, 2020, 2021)
CSAW '20 Applied Research Competition Finalist, *CSAW* (2020)
IMWUT Distinguished Paper Award (2019)
Outstanding New Assistant Professor Award, *Virginia Tech* (2019)
ACM CCS Outstanding Paper Award, *ACM CCS* (2018)
NSF CAREER Award, *NSF* (2018)
Google Faculty Research Award, *Google* (2017-2018)
Assistant Professor Mentoring Award, *Virginia Tech* (2016)
Outstanding Dissertation Award, *UC Santa Barbara* (2016)
Graduate Division Dissertation Fellowship, *UC Santa Barbara* (2015-2016)

SIGMETRICS Best Practical Paper Award, *ACM SIGMETRICS* (2013)
Scholarship for Academic Excellence, *Tsinghua University* (2007-2009)

# PUBLICATIONS

## Refereed Conference Proceedings

1. **[ICWSM '24]** Margie Ruffin, Haeseung Seo, Aiping Xiong, and **Gang Wang**. "Does It Matter Who Said It? Exploring the Impact of Deepfake-Enabled Profiles On User Perception Towards Disinformation." In Proceedings of *The International AAAI Conference on Web and Social Media (ICWSM),* Buffalo, NY, June 2024. (Acceptance rate = TBA)

2. **[CHI '24]** Jaron Mink, Miranda Wei, Collins W. Munyendo, Kurt Hugenberg, Tadayoshi Kohno, Elissa M. Redmiles, and **Gang Wang.** "It's Trying Too Hard To Look Real: Deepfake Moderation Mistakes and Identity-Based Bias." In Proceedings of *ACM CHI Conference on Human Factors in Computing Systems (CHI)*, Honolulu, HI, May 2024. (Acceptance rate = TBA)

3. **[CHI '24]** Chenkai Wang, Zhuofan Jia, Hadjer Benkraouda, Cody Zevnik, Nicholas Heuermann, Roopa Foulger, Jonathan A. Handler, and **Gang Wang.** "VeriSMS: A Message Verification System for Inclusive Patient Outreach against Phishing Attacks." In Proceedings of *ACM CHI Conference on Human Factors in Computing Systems (CHI),* Honolulu, HI, May 2024. (Acceptance rate = TBA)

4. **[WWW '24]** Ying Yuan, Qingying Hao, Giovanni Apruzzese, Mauro Conti, and **Gang Wang.** "Are Adversarial Phishing Webpages a Threat in Reality? Understanding the Users' Perception of Adversarial Webpages." In Proceedings of *The ACM Web Conference (WWW)*, Singapore, May 2024 (**Oral**). (Acceptance rate = 20.2%)

5. **[IEEE SP '24]** Akul Goyal, **Gang Wang**, and Adam Bates. "R-CAID: Embedding Root Cause Analysis within Provenance-based Intrusion Detection." In Proceedings of *The 45th IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2024. (Acceptance rate = TBA)

6. **[ASPLOS '24]** Ali Ahad, **Gang Wang**, Chung Hwan Kim, Suman Jana, Zhiqiang Lin, and Yonghwi Kwon. "FreePart: Hardening Data Processing Software via Framework-based Partitioning and Isolation." In Proceedings of *the ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS),* CA, March 2024. (Acceptance rate = TBA)

7. **[USENIX Security '23]** Xiaojun Xu, Qingying Hao, Zhuolin Yang, Bo Li, David Liebovitz, **Gang Wang**, and Carl Gunter. "How to Cover up Anomalous Accesses to Electronic Health Records." In Proceedings of *the 32nd USENIX Security Symposium (USENIX Security),* Anaheim, CA, August 2023. (Acceptance rate = 29%)

8. **[USENIX Security '23]** Jiahao Yu, Wenbo Guo, Qi Qin, **Gang Wang**, Ting Wang, and Xinyu Xing. "AIRS: Explanation for Deep Reinforcement Learning based Security Applications." In Proceedings of *the 32nd USENIX Security Symposium (USENIX Security),* Anaheim, CA, August 2023. (Acceptance rate = 29%)

9. **[PETS '23]** Faysal Hossain Shezan, Minjun Long, David Hasani, **Gang Wang**, and Yuan Tian. "SenRev: Measurement of Personal Information Disclosure in Online Health Communities." In Proceedings of *Privacy Enhancing Technologies Symposium (PoPETs/PETS),* Lausanne, Switzerland, July 2023. (Acceptance rate = 20%)

10. **[IEEE SP '23]** Jaron Mink, Hadjer Benkraouda, Limin Yang, Arridhana Ciptadi, Ali Ahmadzadeh, Daniel Votipka, and **Gang Wang**. "Everybody's Got ML, Tell Me What Else You Have: Practitioners' Perception of ML-Based Security Tools and Explanations." In Proceedings of *The 44th IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2023. (Acceptance rate = 17.0%)

11. **[IEEE SP '23]** Limin Yang, Zhi Chen, Jacopo Cortellazzi, Feargus Pendlebury, Kevin Tu, Fabio Pierazzi, Lorenzo Cavallaro, and **Gang Wang**. "Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers." In Proceedings of *The 44th IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2023. (Acceptance rate = 17.0%)

12. **[IEEE SP '23]** Yaman Yu, Saidivya Ashok, Smirity Kaushik, Yang Wang, and **Gang Wang**. "Design and Evaluation of Inclusive Email Security Indicators for People with Visual Impairments." In Proceedings of *the 44th IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2023. (Acceptance rate = 17.0%)

13. **[NDSS '23]** Akul Goyal, Xueyuan Han, **Gang Wang**, and Adam Bates**.** "Sometimes, You Aren't What You Do: Mimicry Attacks against Provenance Graph Host Intrusion Detection Systems." In Proceedings of *The Network and Distributed System Security Symposium (NDSS),* San Diego, CA, February 2023. (Acceptance rate = 16.2%)

14. **[GROUP '23]** Margie Ruffin, **Gang Wang**, and Kirill Levchenko. "Explaining Why Fake Photos are Fake: Does It Work?" In Proceedings of *ACM International Conference on Supporting Group Work (GROUP),* Sanibel Island, FL, January 2023. (Acceptance rate = 35.7%)

15. **[USENIX Security '22]** Jaron Mink, Licheng Luo, Natã M. Barbosa, Olivia Figueira, Yang Wang, and **Gang Wang**. "DeepPhish: Understanding User Trust Towards Artificially Generated Profiles in Online Social Networks". In Proceedings of *The 31st USENIX Security Symposium (USENIX Security),* Boston, MA, August 2022 (**Artifacts Available, Artifacts Functional, Results Reproduced**). (Acceptance rate = 18.0%)

16. **[WWW '22]** Chenkai Wang, and **Gang Wang**. "Revisiting Email Forwarding Security under the Authenticated Received Chain Protocol". In Proceedings of *The ACM Web Conference (WWW),* Lyon, France. April 2022. (**Mozilla Bug Bounty $1,000**). (Acceptance rate = 17.7%)

17. **[WWW '22]** Ziyi Zhang, Shuofei Zhu, Jaron Mink, Aiping Xiong, Linhai Song, and **Gang Wang**. "Beyond Bot Detection: Combating Fraudulent Online Survey Takers". In Proceedings of *The ACM Web Conference (WWW),* Lyon, France. April 2022. (Acceptance rate = 17.7%)

18. **[NDSS '22]** Dongliang Mu, Yuhang Wu, Yueqi Chen, Zhenpeng Lin, Chensheng Yu, Xinyu Xing, and **Gang Wang**. "An In-depth Analysis of Duplicated Linux Kernel Bug Reports". In Proceedings of *The Network and Distributed System Security Symposium (NDSS),* San Diego, CA, February 2022. (Acceptance rate = 16.2%)

19. **[IMC '21]** Rishabh Chhabra, Paul Murley, Deepak Kumar, Michael Bailey, and **Gang Wang**. "Measuring DNS-over-HTTPS Performance Around the World". In Proceedings of *The ACM Internet Measurement Conference (IMC)*, Virtual Event, November 2021. (Acceptance rate = 27.5%)

20. **[CCS '21]** Qingying Hao, Licheng Luo, Steve TK Jan, and **Gang Wang**. "It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications". In Proceedings of *The ACM Conference on Computer and Communications Security (CCS)*, Seoul, South Korea, November 2021. (Acceptance rate = 22.2%)

21. **[IMWUT/UbiComp '21]** Natã Miccael Barbosa, **Gang Wang**, Blase Ur, and Yang Wang. "Who Am I? A Design Probe Exploring Real-Time Transparency About Online and Offline User Profiling Underlying Targeted Ads". In Proceedings of *The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp),* September 2021. (Journal article and conference presentation; acceptance rate not provided).

22. **[USENIX Security '21]** Jose Rodrigo Sanchez Vicarte, **Gang Wang**, and Christopher Fletcher. "Double-Cross Attacks: Subverting Active Learning Systems". In Proceedings of *The 30th USENIX Security Symposium (USENIX Security)*, Vancouver, BC, Canada, August 2021. (Acceptance rate = 19.0%)

23. **[USENIX Security '21]** Limin Yang, Wenbo Guo, Qingying Hao, Arridhana Ciptadi, Ali Ahmadzadeh, Xinyu Xing, and **Gang Wang**. "CADE: Detecting and Explaining Concept Drift Samples for Security Applications". In Proceedings of *The 30th USENIX Security Symposium (USENIX Security)*, Vancouver, BC, Canada, August 2021 (**Artifact Evaluated**). (Acceptance rate = 19.0%)

24. **[USENIX Security '21]** Hang Hu, Steve T.K. Jan, Yang Wang, and **Gang Wang**. "Assessing Browser-level Defense against IDN-based Phishing". In Proceedings of *The 30th USENIX Security Symposium (USENIX Security)*, Vancouver, BC, Canada, August 2021. (Acceptance rate = 19.0%)

25. **[USENIX Security '21]** Shinan Liu, Xiang Cheng, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong (Curtis) Zeng, **Gang Wang**, and Yaling Yang. "Stars Can Tell: A Robust Method to Defend against GPS Spoofing using Off-the-shelf Chipset". In Proceedings of *The 30th USENIX Security Symposium (USENIX Security)*, Vancouver, BC, Canada, August 2021 (**Artifact Evaluated**). (Acceptance rate = 19.0%)

26. **[AsiaCCS '21]** Trung Tin Nguyen, Duc Cuong Nguyen, Michael Schilling, **Gang Wang**, and Michael Backes. "Measuring User Perception for Detecting Unexpected Access to Sensitive Resource in Mobile Apps". In Proceedings of The ACM Asia Conference on Computer and Communications Security *(AsiaCCS)*, Hong Kong, China, June 2021. (Acceptance rate = 18.9%)

27. **[NDSS '21]** Junjie Liang, Wenbo Guo, Tongbo Luo, Vasant Honavar, **Gang Wang**, and Xinyu Xing. "FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data". In Proceedings of *The Network and Distributed System Security Symposium (NDSS),* Virtual Conference, February 2021. (Acceptance rate = 15.2%)

28. **[IMWUT/UbiComp '20]** Faysal Hossain Shezan, Hang Hu, **Gang Wang,** and Yuan Tian. "VerHealth: Vetting Medical Voice Applications through Policy Enforcement." In Proceedings of *The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp),* December 2020. (Journal article and conference presentation; acceptance rate not provided).

29. **[USENIX Security '20]** Shuofei Zhu, Jianjun Shi, Limin Yang, Boqin Qin, Ziyi Zhang, Linhai Song, and **Gang Wang**. "Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines". In Proceedings of *The 29th USENIX Security Symposium (USENIX Security)*, Boston, MA, August 2020 (**Artifact Evaluated**). (Acceptance rate = 16.1%)

30. **[IEEE SP '20]** Steve T.K. Jan, Qingying Hao, Tianrui Hu, Jiameng Pu, Sonal Oswal, **Gang Wang**, and Bimal Viswanath. "Throwing Darts in the Dark? Detecting Bots with Limited Data using Neural Data Augmentation". In Proceedings of *The 41st IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2020. (Acceptance rate = 12.3%)

31. **[WWW '20]** Faysal Hossain Shezan, Hang Hu, Jiamin Wang, **Gang Wang**, and Yuan Tian. "Read Between the Lines: An Empirical Measurement of Sensitive Applications of Voice Personal Assistant Systems". In Proceedings of *The Web Conference (WWW),* Taipei, April 2020. (Acceptance rate = 19.2%)

32. **[CCS '19]** Sazzadur Rahaman, **Gang Wang**, and Danfeng Yao. "Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations". In Proceedings of *The 26th ACM Conference on Computer and Communications Security (CCS)*, London, UK, November 2019 (**CSAW '20 Applied Research Competition Finalist**). (Acceptance rate = 16.0%)

33. **[IMC '19]** Mshabab Alrizah, Sencun Zhu, Xinyu Xing, and **Gang Wang.** "Errors, Misunderstandings, and Vulnerabilities: Analyzing the Crowdsourcing Process of Ad-blocking Systems". In Proceedings of *The ACM SIGCOMM Internet Measurement Conference (IMC)*, Amsterdam, Netherlands, October 2019. (Acceptance rate = 19.80%)

34. **[IMC '19]** Peng Peng, Limin Yang, Linhai Song, and **Gang Wang.** "Opening the Blackbox of VirusTotal: Analyzing Online Phishing Scan Engines". In Proceedings of *The ACM SIGCOMM Internet Measurement Conference (IMC)*, Amsterdam, Netherlands, October 2019 (short paper). (Acceptance rate = 19.80%)

35. **[AsiaCCS '19]** Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, and **Gang Wang.** "What Happens After You Leak Your Password: Understanding Credential Sharing on Phishing Sites". In Proceedings of *The 14th ACM Asia Conference on Information, Computer and Communications Security (AsiaCCS)*, Auckland, New Zeland, July 2019. (Acceptance rate = 17.0%)

36. **[USENIX Security '19]** Ying Dong, Wenbo Guo, Yueqi Chen, Xinyu Xing, Yuqing Zhang, and **Gang Wang**. "Towards the Detection of Inconsistencies in Public Security Vulnerability Reports". In Proceedings of *The 28th USENIX Security Symposium (USENIX Security)*, Santa Clara, CA, August 2019. (Acceptance rate = 16.21%)

37. **[IEEE SP '19]** Hang Hu, Peng Peng, and **Gang Wang**. "Characterizing Pixel Tracking through the Lens of Disposable Email Services". In Proceedings of *The 40th IEEE Symposium on Security and Privacy (IEEE SP)*, San Francisco, CA, May 2019. (Acceptance rate = 12.5%)

38. **[IMWUT/UbiComp '19]** Huandong Wang, Yong Li, Sihan Zeng, **Gang Wang**, Pengyu Zhang, Pan Hui, and Depeng Jin. "Modeling Spatio-Temporal App Usage for a Large User Population". In Proceedings of *The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp)*, March 2019. (Journal article and conference presentation; acceptance rate not provided).

39. **[AAAI '19]** Steve T.K. Jan, Joseph Messou, Yen-Chen Lin, Jia-Bin Huang, and **Gang Wang**. "Connecting the Digital and Physical World: Improving the Robustness of Adversarial Attacks". In Proceedings of *The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI)*, Honolulu, HI, January 2019 (**Spotlight**). (Acceptance rate = 16.20%)

40. **[HICSS '19]** Shiliang Tang, Ziming Wu, Xinyi Zhang, **Gang Wang**, Xiaojuan Ma, Haitao Zheng, and Ben Y. Zhao. "Towards Understanding the Adoption and Social Experience of Digital Wallet Systems". In Proceedings of *Hawaii International Conference on System Sciences (HICSS),* Maui HI, January 2019. (Acceptance rate = 48.0%)

41. **[IMC '18]** Ke Tian, Steve T.K. Jan, Hang Hu, Danfeng Yao, and **Gang Wang**. "Needle in a Haystack: Tracking Down Elite Phishing Domains in the Wild". In Proceedings of *ACM Internet Measurement Conference (IMC),* Boston, MA, October 2018. (Acceptance rate = 24.70%)

42. **[CCS '18]** Wenbo Guo, Dongliang Mu, Jun Xu, Purui Su, **Gang Wang**, and Xinyu Xing. "LEMNA: Explaining Deep Learning based Security Applications". In Proceedings of *The 25th ACM Conference on Computer and Communications Security (CCS)*, Toronto, Canada, October 2018 (**Outstanding Paper Award**). (Acceptance rate = 16.60%)

43. **[SecDev '18]** Hang Hu, Peng Peng, and **Gang Wang**. "Towards Understanding the Adoption of Anti-Spoofing Protocols in Email Systems". In Proceedings of *The IEEE Cybersecurity Development Conference (SecDev)*, Cambridge, MA, October 2018. (Acceptance rate = 35.00%)

44. **[IMWUT/UbiComp '18]** Zhen Tu, Runtong Li, Yong Li, **Gang Wang**, Di Wu, Pan Hui, Li Su, and Depeng Jin. "Your Apps Give You Away: Distinguishing Mobile Users by Their App Usage Fingerprints". In Proceedings of *The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp)*, September 2018 (**IMWUT Distinguished Paper Award**). (Journal article and conference presentation; acceptance rate not provided).

45. **[USENIX Security '18]** Hang Hu, and **Gang Wang**. "End-to-End Measurements of Email Spoofing Attacks". In Proceedings of *The 27th USENIX Security Symposium (USENIX Security)*, Baltimore, MD, August 2018. (Acceptance rate = 19.10%)

46. **[USENIX Security '18]** Dongliang Mu, Alejandro Cuevas, Limin Yang, Hang Hu, Bing Mao, Xinyu Xing, and **Gang Wang**. "Understanding the Reproducibility of Crowd-reported Security Vulnerabilities". In Proceedings of *The 27th USENIX Security Symposium (USENIX Security)*, Baltimore, MD, August 2018. (Acceptance rate = 19.10%)

47. **[USENIX Security '18]** Kexiong (Curtis) Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, **Gang Wang**, and Yaling Yang. "All Your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems". In Proceedings of *The 27th USENIX Security Symposium (USENIX Security)*, Baltimore, MD, August 2018. (Acceptance rate = 19.10%)

48. **[AsiaCCS '18]** Xiangwen Wang, Peng Peng, Chun Wang, and **Gang Wang**. "You Are Your Photographs: Detecting Multiple Identities of Vendors in the Darknet Marketplaces". In Proceedings of *The ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, Songdo, Incheon, Korea, June 2018. (Acceptance rate = 20.00%)

49. [**SDM '18**] Huandong Wang, Yong Li, **Gang Wang**, and Depeng Jin. "You Are How You Move: Linking Multiple User Identities from Massive Mobility Traces". In Proceedings of *The SIAM International Conference on Data Mining (SDM)*, San Diego, CA, May 2018. (Acceptance rate = 23.20%)

50. **[CODASPY '18]** Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and **Gang Wang**. "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services". In Proceedings of *The ACM Conference on Data and Applications Security and Privacy (CODASPY)*, Tempe, AZ, March 2018 (short paper). (Acceptance rate = 20.90%)

51. **[NDSS '18]** Huandong Wang, Chen Gao, Yong Li, **Gang Wang**, Depeng Jin, and Jingbo Sun. "De-anonymization of Mobility Trajectories: Dissecting the Gaps between Theory and Practice". In Proceedings of *The 25th Annual Network & Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2018. (Acceptance rate = 20.00%)

52. **[GROUP '18]** Steve T.K. Jan, Chun Wang, Qing Zhang, and **Gang Wang**. "Pay-per-Question: Towards Targeted Q&A with Payments". In Proceedings of *The ACM International Conference on Supporting Group Work (GROUP)*, Sanibel Island, FL, January 2018. (Acceptance rate = 23.40%)

53. **[CIKM '17]** Rupinder Paul Khandpur, Taoran Ji, Steve T.K. Jan, **Gang Wang**, Chang-Tien Lu, and Naren Ramakrishnan. "Crowdsourcing Cybersecurity: Cyber Attack Detection using Social Media". In Proceedings of *The 26th ACM International Conference on Information and Knowledge Management (CIKM)*, Singapore, November 2017. (Acceptance rate = 20.85%)

54. **[CIKM '17]** Huan Yan, Tzu-Heng Lin, **Gang Wang**, Yong Li, Haitao Zheng, Depeng Jin, and Ben Y. Zhao. "On Migratory Behavior in Video Consumption". In Proceedings of *The 26th ACM International Conference on Information and Knowledge Management (CIKM)*, Singapore, November 2017. (Acceptance rate = 20.85%)

55. **[USENIX Security '17]** Fang Liu, Chun Wang, Andres Pico, Danfeng Yao, and **Gang Wang**. "Measuring the Insecurity of Mobile Deep Links of Android". In Proceedings of *The 26th USENIX Security Symposium (USENIX Security)*, Vancouver, Canada, August 2017. (Acceptance rate = 16.28%)

56. **[ICWSM '17]** Xinyi Zhang, Shiliang Tang, Yun Zhao, **Gang Wang**, Haitao Zheng, and Ben Y. Zhao. "Cold Hard E-Cash: Friends and Vendors in the Venmo Digital Payments System". In Proceedings of *International AAAI Conference on Web and Social Media (ICWSM)*, Montreal, Canada, May 2017. (Acceptance rate = 13.73%)

57. **[ICWSM '17]** Huan Yan, Tzu-Heng Lin, **Gang Wang**, Yong Li, Haitao Zheng, Depeng Jin, and Ben Y. Zhao. "A First Look at User Switching Behaviors Over Multiple Video Content Providers". In Proceedings of *International AAAI Conference on Web and Social Media (ICWSM)*, Montreal, Canada, May 2017 (short paper). (Acceptance rate = 19.33%)

58. **[AsiaCCS '17]** Amiangshu Bosu, Fang Liu, Danfeng Yao, and **Gang Wang**. "Collusive Data Leak and More: Large-scale Threat Analysis of Inter-app Communications". In Proceedings of *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, Abu Dhabi, UAE, April 2017. (Acceptance rate = 20.33%)

59. **[IMC '16]** Bolun Wang, Xinyi Zhang, **Gang Wang**, Haitao Zheng, and Ben Y. Zhao. "Anatomy of a Personalized Livestreaming System". In Proceedings of *The 16th ACM SIGCOMM Internet Measurement Conference (IMC),* Santa Monica, CA, November 2016. (Acceptance rate = 25.27%)

60. **[MobiSys '16] Gang Wang,** Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng, and Ben Y. Zhao. "Defending Against Sybil Devices in Crowdsourced Mapping Services". In Proceedings of *The 14th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, Singapore, June 2016. (Acceptance rate = 15.70%)

61. **[ICWSM '16] Gang Wang**, Sarita Schoenebeck, Haitao Zheng, and Ben Y. Zhao. "Will Check-in for Badges: Understanding Bias and Misbehavior on Location-based Social Networks". In Proceedings of *The 10th International AAAI Conference on Web and Social Media (ICWSM)*, Cologne, Germany, May 2016. (Acceptance rate = 17.00%)

62. **[CHI '16] Gang Wang**, Xinyi Zhang, Shiliang Tang, Haitao Zheng, and Ben Y. Zhao. "Unsupervised Clickstream Clustering for User Behavior Analysis". In Proceedings of *SIGCHI Conference on Human Factors in Computing Systems (CHI),* San Jose, CA, May 2016. (Acceptance rate = 23.40%)

63. **[CSCW '15] Gang Wang**, Tianyi Wang, Bolun Wang, Divya Sambasivan, Zengbin Zhang, Haitao Zheng, and Ben Y. Zhao. "Crowds on Wall Street: Extracting Value from Collaborative Investing Platforms". In Proceedings of *The 18th ACM conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*, Vancouver, BC, Canada, March 2015. (Acceptance rate = 28.30%)

64. **[IMC '14] Gang Wang**, Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng, and Ben Y. Zhao. "Whispers in the Dark: Analysis of an Anonymous Social Network". In Proceedings of *The 14th Internet Measurement Conference (IMC),* Vancouver, BC, Canada, November 2014. (Acceptance rate = 22.87%)

65. **[USENIX Security '14] Gang Wang,** Tianyi Wang, Haitao Zheng, and Ben Y. Zhao. "Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers". In Proceedings of *The 23rd USENIX Security Symposium (USENIX Security)*, San Diego, CA, August 2014. (Acceptance rate = 19.14%)

66. **[IMC '13]** Gianluca Stringhini, **Gang Wang**, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Haitao Zheng, and Ben Y. Zhao. "Follow the Green: Growth and Dynamics in Twitter Follower Markets". In Proceedings of *The 13th Internet Measurement Conference (IMC)*, Barcelona, Spain, October 2013. (Acceptance rate = 23.60%)

67. **[USENIX Security '13] Gang Wang**, Tristan Konolige, Christo Wilson, Xiao Wang, Haitao Zheng, and Ben Y. Zhao. "You are How You Click: Clickstream Analysis for Sybil Detection". In Proceedings of *The 22nd USENIX Security Symposium (USENIX Security)*, Washington, DC, August 2013. (Acceptance rate = 16.25%)

68. **[DSN '13] Gang Wang**, Jack Stokes, Cormac Herley, and David Felstead. "Detecting Malicious Landing Pages in Malware Distribution Networks". In Proceedings of *The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Budapest, Hungary, June 2013. (Acceptance rate = 19.62%)

69. **[SIGMETRICS '13]** Xia Zhou, Zengbin Zhang, **Gang Wang**, Xiaoxiao Yu, Ben Y. Zhao, and Haitao Zheng. "Practical Conflict Graphs for Dynamic Spectrum Distribution". In Proceedings of *ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS)*, Pittsburgh, PA, June 2013 (**Best Practical Paper Award**). (Acceptance rate = 13.78%)

70. **[WWW '13] Gang Wang**, Konark Gill, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. "Wisdom in the Social Crowd: An Analysis of Quora". In Proceedings *of The 22nd International World Wide Web Conference (WWW)*, Rio de Janeiro, Brazil, May 2013. (Acceptance rate = 15.04%)

71. **[NDSS '13] Gang Wang**, Manish Mohanlal, Christo Wilson, Xiao Wang, Miriam Metzger, Haitao Zheng, and Ben Y. Zhao. "Social Turing Tests: Crowdsourcing Sybil Detection". In Proceedings of *The 20th Annual Network & Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2013. (Acceptance rate = 18.80%)

72. **[WWW '12] Gang Wang**, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. "Serf and Turf: Crowdturfing for Fun and Profit". In Proceedings of *The 21st International World Wide Web Conference (WWW)*, Lyon, France, April 2012. (Acceptance rate = 12.20%)

73. **[MobiCom '11]** Zengbin Zhang, Xia Zhou, Weile Zhang, Yuanyang Zhang, **Gang Wang**, Ben Y. Zhao, and Haitao Zheng. "I am the Antenna: Accurate Outdoor AP Location using Smartphones". In Proceedings of *The 17th Annual International Conference on Mobile Computing and Networking (MobiCom)*, Las Vegas, NV, September 2011. (Acceptance rate = 13.55%)

## Refereed Journal Articles

74. **[TIST '20]** Huandong Wang, Yong Li, **Gang Wang**, and Depeng Jin. "Linking Multiple User Identities of Multiple Services from Massive Mobility Traces". In *ACM Transactions on Intelligent Systems and Technology (TIST),* 2020.

75. **[TNSM '20]** Huan Yan, Tzu-Heng Lin, **Gang Wang**, Yong Li, Haitao Zheng, Depeng Jin, and Ben Y. Zhao. "On Migratory Behavior in Video Consumption". In *IEEE Transactions on Network and Service Management (TNSM), 2020.*

76. **[TMC '19]** Huandong Wang, Chen Gao, Yong Li, **Gang Wang**, Depeng Jin, and Jingbo Sun. "Anonymization and De-anonymization of Mobility Trajectories: Dissecting the Gaps between Theory and Practice". In *IEEE Transactions on Mobile Computing (TMC),* 2019.

77. **[TON '18] Gang Wang**, Bolun Wang, Tianyi Wang, Ana Nika, Haitao Zheng, and Ben Y. Zhao. "Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services". In *ACM/IEEE Transactions on Networking (TON)*, 2018.

78. **[TSC '18]** Steve T.K. Jan, Chun Wang, Qing Zhang, and **Gang Wang**. "Analyzing Payment-driven Targeted Q&A Systems". In *ACM Transactions on Social Computing (TSC)*, 2018.

79. **[TWEB '17] Gang Wang**, Xinyi Zhang, Shiliang Tang, Christo Wilson, Haitao Zheng, and Ben Y. Zhao. "Clickstream User Behavior Models". In *ACM Transactions on the Web (TWEB)*, 2017.

80. **[TWEB '17]** Tianyi Wang, **Gang Wang**, Bolun Wang, Divya Sambasivan, Zengbin Zhang, Xing Li, Haitao Zheng, and Ben Y. Zhao. "Value and Misinformation in Collaborative Investing Platforms". In *ACM Transactions on the Web (TWEB)*, 2017.

81. **[FCS '15]** Tianyi Wang, Yang Chen, Yi Wang, Bolun Wang, **Gang Wang**, Xing Li, Haitao Zheng, and Ben Y. Zhao. "The Power of Comments: Fostering Social Interactions in Microblog Networks". In *Springer Frontiers of Computer Science (FCS)*, 2015.

82. **[TON '14]** Xia Zhou, Zengbin Zhang, **Gang Wang**, Xiaoxiao Yu, Ben Y. Zhao, and Haitao Zheng. "Practical Conflict Graphs in the Wild". In *ACM Transactions on Networking (TON)*, 2014.

## Refereed Workshop Proceedings

83. **[TCV '24]** Yifan Shen, Zhengyuan Li, and **Gang Wang**. "Practical Region-level Attack against Segment Anything Models." In Proceedings of the *IEEE CVPR Workshop on Fair, Data-efficient, and Trusted Computer Vision (TCV),* in conjunction with IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), Seattle, WA, June 2024 (Acceptance rate not available).

84. **[MLSys '23]** Divyanshu Saxena, Nihal Sharma, Donghyun Kim, Rohit Dwivedula, Jiayi Chen, Chenxi Yang, Sriram Ravula, Zichao Hu, Aditya Akella, Sebastian Angel, Joydeep Biswas, Swarat Chaudhuri, Isil Dillig, Alex Dimakis, Daehyeok Kim, Christopher Rossbach, and **Gang Wang**. "On a Foundation Model for Operating Systems." In Proceedings of *Machine Learning for Systems Workshop (MLSys), in* conjunction with Conference on Neural Information Processing Systems (NeurIPS), New Orleans, LA, December 2023 (Acceptance rate not available).

85. **[DLSP '23]** Zhi Chen, Zhenning Zhang, Zeliang Kan, Limin Yang, Jacopo Cortellazzi, Feargus Pendlebury, Fabio Pierazzi, Lorenzo Cavallaro, and **Gang Wang**. "Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors". In Proceedings of *Deep Learning Security and Privacy Workshop (DLSP*), in conjunction with IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2023. (Acceptance rate = 41.7%).

86. **[WPES '22]** Margie Ruffin, Israel Lopez-Toledo, Kirill Levchenko and **Gang Wang**. "Casing the Vault: Security Analysis of Vault Applications". In Proceedings of *Workshop on Privacy in the Electronic Society (WPES), in* conjunction with ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November 2022. (Acceptance rate = 33.8%).

87. **[DLS '21]** Limin Yang, Arridhana Ciptadi, Ali Ahmadzadeh, and **Gang Wang**. "BODMAS: An Open Dataset for Learning based Temporal Analysis of PE Malware". In Proceedings of *Deep Learning and Security Workshop (DLS), in* conjunction with IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2021. (Acceptance rate = 40.0%).

88. **[SafeThings '20]** Hang Hu, Limin Yang, Shihan Lin, and **Gang Wang**. "A Case Study of the Security Vetting Process of

Smart-home Assistant Applications". In Proceedings of *IEEE Workshop on the Internet of Safe Things (SafeThings)*, in conjunction with IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 2020. (Acceptance rate not available)

89. **[SafeConfig '17]** Alexander Kedrowitsch, Danfeng Yao, **Gang Wang**, and Kirk Cameron. "A First Look: Using Linux Containers for Deceptive Honeypots". In Proceedings of *Applying the Scientific Method to Active Cyber Defense Research (SafeConfig)*, in conjunction with the ACM Conference on Computer and Communications Security (CCS), Dallas, USA, October 2017. (Acceptance rate = 50%)

90. **[MoST '17]** Fang Liu, Haipeng Cai, **Gang Wang**, Danfeng Yao, Karim O. Elish, and Barbara G. Ryder. "MR-Droid: A Scalable and Prioritized Analysis of Inter-App Communication Risks". In Proceedings of *Mobile Security Technologies (MoST)*, in conjunction with IEEE Symposium on Security and Privacy (SP), San Jose, CA, May 2017. (Acceptance rate = 33.33%)

91. **[HotNets '13]** Zengbin Zhang, Lin Zhou, Xiaohan Zhao, **Gang Wang**, Yu Su, Miriam Metzger, Haitao Zheng, and Ben Y. Zhao. "On the Validity of Geosocial Mobility Traces". In Proceedings of *ACM Workshop on Hot Topics in Networks (HotNets)*, College Park, MD, November 2013. (Acceptance rate = 23.64%)

92. **[HotMobile '11]** Christo Wilson, Troy Steinbauer, **Gang Wang**, Alessandra Sala, Haitao Zheng, and Ben Y. Zhao. "Privacy, Availability and Economics in the Polaris Mobile Social Network". In Proceedings of *The 12th ACM Workshop on Mobile Computing Systems and Applications (HotMobile)*, Phoenix, AZ, March 2011. (Acceptance rate = 32.65%)

93. **[P2PNet '09] Gang Wang**, Shining Wu, Guodong Wang, Beixing Deng, and Xing Li. "Experimental Study on Neighbor Selection Policy for Phoenix Network Coordinate System." In Proceedings of *IEEE International Workshop on Peer-To-Peer Networking (P2PNet)*, St. Petersburg, Russia, 2009. (Acceptance rate = 38.0%)

## Refereed Posters and Demos

94. **[IEEE SP '23]** Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Gang Wang, and Adam Bates. "How do Endpoint Detection Products Make Use of MITRE ATT&CK?" *The 44th IEEE Symposium on Security and Privacy (IEEE SP),* San Francisco, CA, May 2023.

95. **[CCS '20]** Shuofei Zhu, Ziyi Zhang, Limin Yang, Linhai Song, and **Gang Wang**. "Demonstration: Benchmarking Label Dynamics of VirusTotal Engines". *ACM Conference on Computer and Communications Security (CCS)*, Virtual Conference, November 2020.

96. **[SIGSPATIAL '17]** Qihang Gu, Dimitris Sacharidis, Michael Mathioudakis, and **Gang Wang**. "Inferring Venue Visits from GPS Trajectories". In Proceedings of *the 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (SIGSPATIAL),* New York, NY, November 2017.

97. **[EuroS&P '17]** Amiangshu Bosu, Fang Liu, Danfeng Yao, and **Gang Wang**. "Android Collusive Data Leaks with Flow-sensitive DIALDroid Dataset". IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, April 2017.

98. **[SIGCOMM '13]** Tianyi Wang, **Gang Wang**, Xing Li, Haitao Zheng, and Ben Y. Zhao. "Characterizing and Detecting Malicious Crowdsourcing". *ACM Special Interest Group on Data Communication (SIGCOMM),* Hong Kong, China, August 2013.

99. **[DySpan '12]** Xia Zhou, Zengbin Zhang, **Gang Wang**, Xiaoxiao Yu, Ben Y. Zhao, and Haitao Zheng. "Measurement-calibrated conflict graphs for dynamic spectrum distribution". *ACM 2012 IEEE International Symposium on Dynamic Spectrum Access Networks (DySpan), Bellevue, WA, October 2012*.

## Patents

100. Bimal Viswanath, Arik Hadass, Sonal Oswal, Jiameng Pu, Tianrui Hu, **Gang Wang**, Steve Jan, Qingying Hao. "A Method to Detect Web Bots with Limited Data Using Neural Networks". Filed by VTIP. IP Disclosure: 02/04/2020. # VTIP 20-061.

101. Yaling Yang, Shinan Liu, **Gang Wang**. "A Low-Cost GPS Spoofing Detector and Spoofer Localizer". Filed by VTIP. IP Disclosure: 03/03/2020. # VTIP 20-070. U.S. Patent Application No. 63/047,085.

102. Yaling Yang, Yuancao Shu, Shinan Liu, **Gang Wang**, Kexiong Zeng. "GPS Spoofing Tool to Road Navigation System". Filed by VTIP. IP Disclosure: 09/12/2018. # VTIP 19-026.

103. **Gang Wang**, Jack Stokes, Cormac Herley, and David Felstead. "Identifying Web Pages In Malware Distribution

Networks". Filed by Microsoft Corporation, published on 07/03/2014. Pattern #: US 2014/0189864 A1.

### Book Chapters

104. Wenbo Guo, Jun Xu, **Gang Wang**, and Xinyu Xing. "Explaining Deep Learning Based Security Applications." In: Wang, C., Iyengar, S., Sun, K. (eds) *Embedded Assurance for Cyber Systems*, 2023. Springer, Cham. https://doi.org/10.1007/978-3-031-42637-7_12

## PROFESSIONAL ACTIVITIES

### Technical Program Committee

- **[USENIX Security]** USENIX Security Symposium: 2018, 2021, 2022, 2023, 2024
- **[IEEE SP]** IEEE Symposium on Security and Privacy: 2022, 2023, 2024, 2025
- **[CCS]** The ACM Conference on Computer and Communications Security: 2021, 2022, 2023, 2024
- **[NDSS]** The Network and Distributed System Security Symposium: 2020, 2021, 2022, 2023, 2024
- **[EuroS&P]** IEEE European Symposium on Security and Privacy: 2024
- **[IMC]** ACM Internet Measurement Conference: 2019, 2024
- **[MobiSys]** ACM International Conference on Mobile Systems, Applications, and Services: 2020, 2021, 2023
- **[EthiCS]** International Workshop on Ethics in Computer Security: 2023
- **[WWW]** The Web Conference or TheWebConf ("Security, Privacy, and Trust" Track): 2017, 2019, 2020, 2021, 2022, 2024
- **[RAID]** International Symposium on Research in Attacks, Intrusions and Defenses: 2021, 2022
- **[DIMVA]** Conference on Detection of Intrusions and Malware & Vulnerability Assessment: 2021, 2022
- **[DLS]** Deep Learning and Security Workshop, 2021
- **[SafeThings]** IEEE/ACM Workshop on the Internet of Safe Things, 2023
- **[WiSec]** ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2021
- **[DSN]** IEEE/IFIP International Conference on Dependable Systems and Networks, 2020
- **[ACSAC]** Annual Computer Security Applications Conference: 2018, 2019, 2020, 2021, 2023
- **[CNS]** IEEE Conference on Communications and Network Security: 2019
- **[ICWSM]** AAAI International Conference on Web and Social Media: 2016, 2017, 2018, 2019, 2022
- **[eCrime]** APWG Annual Symposium on Electronic Crime Research: 2018, 2019, 2020
- **[ICICS]** International Conference on Information and Communications Security: 2021
- **[AISec]** ACM Workshop on Artificial Intelligence and Security: 2016, 2017, 2018, 2019, 2020, 2021
- **[MLBA]** IJCAI Workshop on Machine Learning for Binary Analysis, 2020
- **[WACCO]** Workshop on Attackers and Cyber-Crime Operations: 2019, 2020, 2021
- **[CSCW]** ACM Conference on Computer-Supported Cooperative Work and Social Computing: 2018
- **[IEEE SP-S]** IEEE Symposium on Security and Privacy (Student PC): 2016

### Journal Reviewer

- **[IMWUT]** The Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies: 2021
- **[TDSC]** IEEE Transactions on Dependable and Secure Computing: 2016, 2017, 2018, 2019, 2022
- **[TWEB]** ACM Transactions on the Web: 2017, 2018
- **[TIFS]** Transactions on Information Forensics & Security: 2018
- **[SP]** IEEE Security & Privacy: 2018, 2019, 2022
- **[Frontiers]** Frontiers in ICT: 2018
- **[TMC]** Transactions on Mobile Computing: 2017
- **[IEEE Communications]** IEEE Communications Magazine: 2017
- **[TOIT]** ACM Transactions on Internet Technology: 2017
- **[LOS ONE]** Public Library of Science Open Access Journal: 2017
- **[Science Advances]** AAAS Open Access Journal: 2017
- **[JASIST]** Journal of the Association for Information Science and Technology: 2016
- **[TIST]** ACM Transactions on Intelligent Systems and Technology: 2015
- **[TWireless]** IEEE Transactions on Wireless Communications: 2015
- **[COMNET]** Journal on Computer Networks, special issue on P2P Network Measurement: 2011

### Journal Guest Editor

- **[WWWJ]** World Wide Web, Special issue on “Social computing and big data applications”: 2017, 2018, 2019

### Conference/Workshop Organization

- **[IEEE SP]** IEEE Symposium on Security and Privacy: Workshops Co-Chair, 2024
- **[MobiSys]** ACM International Conference on Mobile Systems, Applications, and Services: Travel Grant Chair, 2023
- **[KDD AI4Cyber-MLHat]**AI-enabled Cybersecurity Analytics and Deployable Defense: General Chair, 2022
- **[KDD MLHat]** International Workshop on Deployable Machine Learning for Security Defense: General Chair, 2021
- **[KDD MLHat]** International Workshop on Deployable Machine Learning for Security Defense: General Chair, 2020

### Other Services

- **[NSF]** National Science Foundation (NSF) Review Panel (×1): 2023
- **[NSF]** SaTC PI Meeting: Breakout Session Co-lead (AI for Security): 2022
- **[NSF]** National Science Foundation (NSF) Review Panel (×1): 2022
- **[NSF]** National Science Foundation (NSF) Review Panel (×2): 2021
- **[NSF]** National Science Foundation (NSF) Review Panel (×1): 2019
- **[NSF]** National Science Foundation (NSF) Review Panel (×3): 2018
- **[UNIPD]** University of Padova Internal Proposal Review Panel: 2018

## GRANTS

Institute for Artificial Cyber Threat Intelligence and OperatioN (ACTION)

- **My Role: Co-PI**
- PI: Giovanni Vigna
- UIUC share (with Bo Li): $1,296,750
- Personal Share: $646,537 (50% of UIUC share)
- Total: $20,000,000
- NSF
- 06/01/2023 - 05/31/2028

Scalable Continuous Remote Attestation for Multi-Cloud

- **My Role: PI**
- Co-PI: Kirill Levchenko
- Personal Share: $105,939 (50%)
- Total: $211,878
- IBM
- 08/16/2023 - 08/15/2025

Foundation-Model-Driven Resilience for Cloud Computing

- **My Role: Co-PI**
- PI: Ravishankar K Iyer; Other Co-PIs: Zbigniew T Kalbarczyk, Phuong Cao, Bill Kramer
- Personal Share: $139,935 (20%)
- Total: $699,679
- IBM
- 08/16/2023 - 08/15/2025

High Trust Patient Outreach

- **My Role: PI**
- Co-PIs: Jonathan Handler, Roopa Foulger, Nick Heuermann, Cody Zevnik
- Personal Share: $29,304 (39%)
- Total: $74,340
- Jump ARCHES
- 01/18/2022 to 01/17/2023

Protecting Critical Infrastructures Against Evolving Insider Threats

- **My Role: Co-PI**
- PI: Carl A. Gunter; other Co-PIs: Bo Li

- Personal Share: $89,230 (33%)
- Total: $270,396
- C3.ai Digital Transformation Institute
- 06/01/2022 to 05/31/2023

SaTC: CORE: Small: Collaborative: Towards Label Enrichment and Refinement to Harden Learning-based Security Defenses

- **My Role: PI**
- Co-PI: Xinyu Xing
- Personal Share: $250,000 (50%)
- Total: $500,000
- National Science Foundation (NSF)
- 10/01/2021 to 09/30/2024

Hybrid Cloud: Cross-layer AI-driven Resiliency and Security

- **My Role: PI**
- Co-PIs: Ravishankar Iyer, and Zbigniew Kalbarczyk
- Personal Share: $205,606 (from IBM) + $51,401 (UIUC cost share) (33.3%)
- Total: $616,818 (from IBM) + $154,204 (UIUC cost share)
- IBM
- 08/24/2021 to 08/24/2023

SaTC: CORE: Medium: Principled Foundations for the Design and Evaluation of Graph-Based Host Intrusion Detection Systems

- **My Role: Co-PI**
- PI: Adam Bates
- Personal Share: $600,599 (50%)
- Total: $1,201,199
- National Science Foundation (NSF)
- 10/01/2021 to 09/30/2025

Combating Concept Drift in Security Applications via Proactive Data Synthesis

- **My Role: Sole PI**
- Personal Share: $70,000 + $10,000 AWS credits (100%)
- Total: $70,000 + $10,000 AWS credits
- Amazon Research Awards (AI for Information Security)
- 04/01/2021 to 03/30/2022

SaTC: CORE: Small: Collaborative: Towards Facilitating Kernel Vulnerability Reproduction by Fusing Crowd and Machine Generated Data

- **My Role: Co-PI**
- PI: Xinyu Xing
- Personal Share: $175,000 (35%)
- Total: $500,000
- National Science Foundation (NSF)
- 10/01/2020 to 09/30/2023

CAREER: Machine Learning Assisted Crowdsourcing for Phishing Defense.

- **My Role: Sole PI**
- Personal Share: $538,522 (100%)
- Total: $538,522
- National Science Foundation (NSF)
- 06/01/2018 to 05/31/2023

Augmenting User-level Defense Against Email Spoofing Attacks.

- **My Role: Sole PI**
- Personal Share: $54,735 (100%)
- Total: $54,735
- Google Faculty Award
- 03/15/2018 to 03/14/2019

SaTC: CORE: Small: Securing Web-to-Mobile Interface Through Characterization and Detection of Malicious Deep Links.

- **My Role: PI**
- Co-PI: Danfeng Yao
- Personal Share: $400,000 (80%)
- Total: $500,000
- National Science Foundation (NSF)
- 08/01/2017 to 07/31/2021

## SELECTED PRESS

- **[Financial Times]** Is artificial intelligence the solution to cyber security threats? 1/2024
- **[The Wall Street Journal]** Vans, North Face Parent VF Warns Cyberattack May Snarl Holiday Deliveries. 12/2023
- **[The Washington Post]** AI fake nudes are booming. It's ruining real teens' lives. 11/2023
- **[Bloomberg]** AI-Made Deepfake Political Ads Targeted by Michigan Lawmakers. 10/2023
- **[Rappler]** When creative work becomes a target of review bombing, what do platforms do? 09/2023
- **[Spectrum News]** 'Scammers' threaten quality of research survey data. 08/2023
- **[Futurum]** Can you trust what you see online? 04/2023
- **[Scholarly Communication]** Write it Down: Writing as a Step Toward Better Research. 01/2023
- **[WLS Radio, WGN Radio, WGN-TV]** Radio/TV Interview on Cyber Warfare. 03/2022
- **[New Scientist]** People are bad at spotting fake LinkedIn profiles generated by AI. 02/2022
- **[APNIC]** Measuring DNS-over-HTTPS performance around the world. 02/2022
- **[WCIA News]** Russian cyberattacks are "real threat." 02/2022
- **[WNIJ NPR]** Fallout From The Ransomware Attack At Illinois Valley Community College Is Still Far From Over. 09/2020
- **[Vox]** Why coronavirus scammers can send fake emails from real domains. 04/2020
- **[The Daily Illini]** Campus bluetooth attendance tracking raises debate. 01/2020
- **[Bloomberg]** How Hackers Can Take Over Your Car's GPS. 06/2019
- **[The Cyberwire podcast]** Driving GPS manipulation. 10/2018
- **[The Wall Street Journal]** How to Defend Against GPS Spoofing Attacks. 09/2018
- **[Forbes]** This GPS Spoofing Hack Can Really Mess Up Your Google Maps Trips. 07/2018
- **[ACM TechNews]** Researchers Mount Successful GPS Spoofing Attack Against Road Navigation Systems. 07/2018
- **[The Register]** Sad Nav: How a cheap GPS spoofer gizmo can tell drivers to get lost. 07/2018
- **[Naked Security]** How to spoof someone's GPS navigation to send them the wrong way. 07/2018
- **[The Cyberwire podcast]** Measuring the spear phishing threat. 07/2018
- **[ACM TechNews]** Meeting Updated Phishing Attacks Head On. 06/2018
- **[Science Daily]** Extra vigilance required to combat growing sophistication of phishing attacks. 06/2018
- **[Daily Mail]** Most popular passwords of 2017 are revealed, and they are incredibly easy to crack. 05/2018
- **[Daily Express]** Worst passwords revealed: If yours is on this list, you should change it right now. 05/2018
- **[Dark Reading]** More Than Half of Users Reuse Passwords. 05/2018
- **[Yahoo! News]** From "Superman" to "Liverpool" Have you got one of 2018's worst passwords. 05/2018
- **[Security Magazine]** Why People are "Password Walking". 05/2018
- **[Mirror]** The most common passwords of 2017 – and they're worryingly easy to guess. 05/2018
- **[The Sun]** Most common passwords revealed: are you guilty of using these hilariously terrible picks. 05/2018
- **[New Scientist]** Most people re-use old passwords (but you don't, right). 01/2018
- **[The New York Times]** Alexa, What Happened to My Car. 03/2018
- **[CNN]** Online holiday shopping scams to watch out for. 11/2017
- **[WVTF Radio/NPR]** Now You Really Wanna Cry. 05/2017
- **[phys.org]** Android apps can conspire to mine information from your smartphone. 04/2017
- **[The Hill]** Thousands of Android apps can "collude" to leak information, research shows. 04/2017
- **[The Sun]** Your smartphone apps are "secretly colluding" to spy on you in terrifying detail, researchers warn. 04/2017
- **[Business Insider]** Android apps can breach and share your personal data. 04/2017
- **[New Scientist]** Android apps share data between them without your permission. 04/2017
- **[Independent]** Android apps secretly steal users' data by colluding with each other, finds research. 04/2017
- **[Daily Mail]** Android apps are "secretly colluding" to spy on the private lives of millions of users. 04/2017
- **[ACM TechNews]** Android apps can conspire to mine information from your smartphone. 04/2017
- **[live24News]** Google Android Apps Swap Information Without Your Own Permission. 04/2017

- **[WVTF Radio/NPR]** Internet Scams, Hacks and Malware: A Cat & Mouse Game. 01/2017
- **[Fusion]** If You Use Waze, Hackers Can Stalk You. 04/2016
- **[Channel 10 CBS News]** Hackers can stalk you via Waze app. 04/2016
- **[Recode/CNBC]** Google's Waze says, Nope, hackers can't stalk you on. 04/2016
- **[Fusion]** Waze comes up with a fix for hack that let researchers track users' movements. 04/2016
- **[Tech Times]** Vulnerability In Popular Waze Navigation App Could Let Hackers Stalk You In Real Time. 04/2016
- **[Tech Crunch]** Waze downplays exploit that let researchers track users. 04/2016
- **[Fortune]** Here's How Google's Waze Can Reportedly Be Used to Stalk Drivers. 04/2016
- **[i24 News]** U.S. Researchers Expose "Waze" Security Lapse. 04/2016
- **[NakedSecurity]** How to prevent snoops from stalking you in Waze with "ghost" drivers. 04/2016
- **[TechNewsToday]** Waze Hackers Have You in Their Sights. 04/2016
- **[Infosecurity Magazine]** Waze App: The Road to Stalking Drivers. 04/2016
- **[Android Headlines]** Hackers Can Exploit Waze to Track Drivers in Real Time. 04/2016
- **[LA Times]** At Whisper's news-gathering operation, data collection comes under siege. 10/2014
- **[MIT Technology Review]** Fake Followers for Hire, and How to Spot Them. 10/2014
- **[Boston Globe]** A Dark Force, Unleashed Online. 01/2012
- **[The Consumerist]** Growing Number of Cyber Shills Invade Online Reviews. 12/2011
- **[InfoWorld]** Cyber Shill Business Is Booming. 12/2011
- **[Slashdot]** Million Dollar Crowdturfing Industry Dupes Social Networks. 12/2011
- **[MIT Technology Review]** Hidden Industry Dupes Social Media Users. 12/2011

# TALKS

- Using ML in Security Operations Centers: Human and Data Perspectives
  *NSF Workshop on Automating Cyber Response, Seymour Marine Discovery Center, Santa Cruz, CA (March 2024)*
- AI for Offense: What Does It Mean for Disinformation and Social Engineering?
  *AI and Security CoP: External Speaker Series, Intel, Virtual (February 2024)*
- Understanding Deepfake-based Social Engineering: from Users' Perspectives
  *Inaugural Faculty Lecture Series, Alumni Relations Event, Illini Center, Chicago, IL (October 2023)*
- Open Challenges of Malware Detection under Concept Drift
  *Keynote speech at ACM Workshop on Robust Malware Analysis (WoRMA), Virtual (May 2022)*
- Security Panel: Promises and challenges of Security in Trustworthy AI
  *The 5th Deep Learning and Security Workshop, Virtual (May 2022)*
- Post-PhD Career Panel: Paths Not Yet Taken + An Insider View of Academic Hiring
  *PhD Career Day Workshop, The University of Chicago, Chicago, IL (May 2022)*
- Online Deception in the Age of Machine Learning
  *Privacy and Security in ML Seminars (PriSec-ML), University College London, UK, Virtual (March 2022)*
- Combating Online Deception in the Age of Machine Learning
  *Distinguished Lecture Series, CISPA Helmholtz Center for Information Security, German, Virtual (December 2021)*
- Assessing Browser-level Defense against IDN-based Phishing
  *The 30th USENIX Security Symposium, Vancouver, BC, Canada, Virtual (August 2021)*
- Detecting, Explaining, and Labeling Concept Drift Samples for Security Applications
  *C3SR IBM-ILLINOIS Center for Cognitive Computing Systems Research Faulty Meeting, Virtual (March 2021)*
- The Art of Impersonation: Demystifying Spear Phishing Attacks.
  *Women in Computer Science (WCS) Explore CS Series, Virtual (October 2020)*
- Data-Driven Security Applications: Case Studies and Open Questions.
  *Illinois Cyber Scholars Program (ICSSP) Seminar, Virtual (October 2020)*
- Data-Driven Security Applications: Case Studies and Open Questions.
  *Department of Electronic Engineering, Tsinghua University, Beijing, China (June 2020)*
- Data-Driven Security Applications: Case Studies and Open Questions.
  *Blue Hexagon, Sunnyvale CA (January 2020)*

- Trustworthiness of Information Sources (Panel)
  *DARPA Workshop: Multi-Modal Understanding and Summarization (MuMUS) of Critical Events*
  *The University of Pennsylvania, Philadelphia PA (October 2019)*
- Machine Learning Assisted Crowdsourcing for Phishing Defense.
  *Cybersecurity Technology Transition to Practice Workshop, Chicago, IL (July 2019)*
- Human Augmentation for Internet Security.
  *The Center of Cyber Defense and Network Assurability (CyberDNA), UNC Charlotte, Charlotte NC (May 2019)*
- Human Augmentation for Internet Security.
  *Department of Computer Science, University of Southern California, Los Angeles, CA (March 2019)*
- Human Augmentation for Internet Security.
  *Department of Computer Science, University of Virginia, Charlottesville, VA (March 2019)*
- Rethinking Human Factors for Online Security.
  *Department of Computer Science, Dartmouth College, Hanover, NH (February 2019)*
- Human Augmentation for Internet Security.
  *Department of Computer Science, The University of Chicago, Chicago, IL (February 2019)*
- Human Augmentation for Internet Security.
  *College of Information Sciences and Technology, The Penn State University, University Park, PA (February 2019)*
- Human Augmentation for Internet Security.
  *Department of Computer Science, Purdue University, West Lafayette, IN (January 2019)*
- Human Augmentation for Internet Security.
  *Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN (January 2019)*
- Human Augmentation for Internet Security.
  *Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL (December 2018)*
- Exploitable Human Factors and Their Implications for Online Security.
  *Department of Computer Science, Dartmouth College, Hanover, NH (May 2018)*
- The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services.
  *ACM Conference on Data and Applications Security and Privacy, Tempe, AZ (March 2018)*
- Measuring the Insecurity of Mobile Deep Links of Android.
  *USENIX Security Symposium (USENIX Security), Vancouver, Canada (August 2017)*
- Identity Abuse in Mobile Social Networks and Email Systems.
  *Institute for Creativity, Arts, and Technology, Virginia Tech, Blacksburg, VA (August 2017)*
- Sybil Devices in Crowdsourced Mapping Services.
  *Workshop on Data and Algorithmic Transparency, New York City, NY (November 2016)*
- Human Factors in the Security of Online and Mobile Systems.
  *Virginia Tech CS Graduate Seminar, Blacksburg, VA (September 2016)*
- "Will Check-in for Badges": Understanding Bias and Misbehavior on Location-based Social Networks.
  *International AAAI Conference on Web and Social Media, Cologne, Germany (May 2016)*
- Unsupervised Clickstream Clustering for User Behavior Analysis.
  *SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA (May 2016)*
- Human Factors in the Security of Online Systems.
  *Department of Computer Science, Stony Brook University, Stony Brook, NY (April 2016)*
- Human Factors in the Security of Online Systems.
  *Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL (March 2016)*
- Human Factors in the Security of Online Systems.
  *Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL (March 2016)*
- Human Factors in the Security of Online Systems.
  *Department of Computer Science, University of Minnesota, Minneapolis, MN (March 2016)*
- Human Factors in the Security of Online Systems.

*Department of Computer Science, The Ohio State University, Columbus, OH (February 2016)*

- Human Factors in the Security of Online Systems.  
  *Department of Computer Science, Virginia Tech, Blacksburg, VA (February 2016)*
- Attacks and Defenses in Large Online Communities.  
  *Uber Inc., San Francisco, CA (February 2016)*
- Attacks and Defenses in Large Online Communities.  
  *LinkedIn Inc., Mountain View, CA (December 2015)*
- Whispers in the Dark: Analysis of an Anonymous Social Network.  
  *The 14th Internet Measurement Conference, Vancouver, BC, Canada (November 2014)*
- Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers.  
  *Microsoft Membership PM R&D Team, Redmond, WA (*September 2014*)*
- Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers.  
  *Microsoft Azure Data Science and Security Team, Redmond, WA (August 2014)*
- Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers.  
  *The 23rd USENIX Security Symposium, San Diego, CA (August 2014)*
- Man vs. Machine: Practical Adversarial Detection of Malicious Crowdsourcing Workers.  
  *UW-MSR Summer Institute, Seattle, WA (July 2014)*
- Wisdom in the Social Crowd: An Analysis of Quora.  
  *The 22nd International World Wide Web Conference, Rio de Janeiro, Brazil (May 2013)*
- You are How You Click: Clickstream Analysis for Sybil Detection.  
  *The 22nd USENIX Security Symposium, Washington, DC, WA (August 2013)*
- You are How You Click: Clickstream Analysis for Sybil Detection.  
  *Security Team of Renren Inc., Beijing, China (May 2013)*
- Social Turing Tests: Crowdsourcing Sybil Detection.  
  *The 20th Annual Network & Distributed System Security Symposium, San Diego, CA (February 2013)*
- Fighting Fire with Fire: Crowdsourcing Security Threats and Solutions on the Social Web.  
  *AT&T Security Research Center, Middletown, NJ (January 2013)*
- Serf and Turf: Crowdturfing for Fun and Profit.  
  *The 21st International World Wide Web Conference, Lyon, France (April 2012)*

## CODE AND DATA RELEASE

- **[BODMAS Malware Data]** A dataset containing timestamped malware samples and well-curated family information: 57,293 malware samples and 77,142 benign samples collected from 2019 to 2020 (581 families), 2021  
  https://whyisyoung.github.io/BODMAS/
- **[DoH]** A tool to conduct DNS-over-HTTPS (DoH) performance measurements (resolution time), 2021  
  https://github.com/rishabhc/imc21-measuring-doh-performance
- **[pHashingAdv]** Open-sourced code and dataset for adversarial attacks against perceptual hashing, 2021  
  https://gangw.cs.illinois.edu/hash.html
- **[CADE]** A tool to detect concept drift samples for security applications, 2021  
  https://github.com/whyisyoung/CADE
- **[GPS Anti-spoofing Tool]** A mobile app to detect GPS spoofing using off-the-shelf chipsets, 2021  
  https://github.com/shinan6/robust-gps-antispoofing
- **[VirusTotal Data]** Dataset of the daily snapshots of VirusTotal labels for 14,000 files over a year, 2020  
  https://sfzhu93.github.io/projects/vt/index.html
- **[VPA Data]** Dataset of sensitive commands for Amazon Alexa and Google Homes, 2020  
  https://github.com/faysalhossain2007/Read-Between-the-Lines-An-Empirical-Measurement-of-Sensitive-Applications-of-Voice-Personal-Assista
- **[PCI-Checker]** A light-weight vulnerability scanner for e-commerce websites, 2019  
  https://github.com/sazzad114/pci-checker
- **[BuggyCart]** A customizable testbed to assess the performance of PCI vulnerability scanners, 2019

https://github.com/sazzad114/buggycart

- **[VIEM]** An NLP tool to extract vulnerability information from unstructured vulnerability reports, 2019
https://github.com/pinkymm/inconsistency_detection
- **[AdvPhyML]** The implementation of a method to generate physical domain adversarial examples, 2019
https://github.com/stevetkjan/Digital2Physical
- **[LEMNA]** A machine learning explanation system to security applications, 2018
https://github.com/Henrygwb/Explaining-DL
- **[SquatPhish]** A collection of toolkits to detect phishing websites that have squatting domains, 2018
https://github.com/SquatPhish
- **[MemoryVul Data]** 368 memory corruption vulnerabilities with PoC exploits and docker images, 2018
https://github.com/VulnReproduction/LinuxFlaw
- **[Password Data]** A collection of 107 password datasets (61.5 million passwords), 2018
https://gangw.cs.illinois.edu/pass.html
- **[De-anonyLoc]** A toolkit of 7 de-anonymization algorithms for location data. 2018
https://github.com/whd14/De-anonymization-of-Mobility-Trajectories
- **[Clickstream Viz]** A ML tool to cluster and visualize clickstreams for user behavior analysis, 2016
http://cs.ucsb.edu/~xyzhang/clickstream/index.html

# TEACHING

- CS 562: Advanced Topics in Security, Privacy, and Machine Learning, *UIUC*, Instructor, Fall 2023.
- CS 463: Computer Security II, *UIUC*, Instructor, Spring 2023.
- CS 463: Computer Security II, *UIUC*, Instructor, Fall 2022.
- CS 463: Computer Security II, *UIUC*, Instructor, Fall 2021.
- CS 463: Computer Security II, *UIUC*, Instructor, Spring 2021.
- CS 598: Machine Learning for Sys, Networks, and Security, *UIUC,* Instructor, Fall 2020.
- CS 463: Computer Security II, *UIUC*, Instructor, Spring 2020.
- CS 598: Machine Learning for Sys, Networks, and Security, *UIUC,* Instructor, Fall 2019.
- CS 4264: Principles of Computer Security, *Virginia Tech,* Instructor, Spring 2019.
- CS 4984: Web Applications Security, *Virginia Tech,* Instructor, Fall 2018.
- CS 4264: Principles of Computer Security, *Virginia Tech,* Instructor, Spring 2018.
- CS 6604: Applied Machine Learning in Security, *Virginia Tech,* Instructor, Fall 2017.
- CS 4264: Principles of Computer Security, *Virginia Tech*, Instructor, Fall 2016.
- CS 290F: Smartphone-centric Systems and Applications, *UCSB*, Guest Lecturer, Fall 2015.
- CS 276: Graduate Networking, *UCSB*, Teaching Assistant, Fall 2011.
- CS 176B: Network Computing, *UCSB*, Teaching Assistant, Spring 2011.
- CS 64: Computer Organization, *UCSB*, Teaching Assistant, Winter 2011.
- CS 40: Foundations of Computer Science, *UCSB*, Teaching Assistant, Fall 2010.

# INTERNAL SERVICES

- Security and Privacy Area Chair (CS), *UIUC,* 2023-2024
- Undergraduate Student Awards Committee, *UIUC*, 2023-2024
- HackIllinois 2023, Hackathon Mentor, 2023
- Undergraduate Student Awards Committee (Chair), *UIUC*, 2022-2023
- Grad Admission, *UIUC*, 2022-2023
- Panelist: Research Experience for Undergraduates (REU) program ("Mentors, Advisors, and Sponsors"), *UIUC*, 2022
- Undergraduate Student Awards Committee, *UIUC*, 2021-2022
- FAA Committee (Grad Admission), *UIUC*, 2021-2022
- Capricious Grading Committee, *UIUC,* 2021-2022
- Undergraduate Student Awards Committee, *UIUC*, 2020-2021
- FAA Committee (Grad Admission), *UIUC*, 2020-2021
- Security Analysis Team for the Safer Illinois App, *UIUC*, 2020
- Panelist: Research Experience for Undergraduates (REU) program ("Graduate School"), *UIUC*, 2020
- Graduate Studies Committee, *UIUC*, 2019-2020

- Undergraduate Student Awards Committee, *UIUC*, 2019-2020
- Graduate Admission Committee, *Virginia Tech*, 2018-2019
- PhD Qualifier in Systems, Networking, and Cybersecurity (SNC) Committee, *Virginia Tech*, 2018-2019
- Graduate Admission Committee, *Virginia Tech*, 2017-2018
- PhD Qualifier in Systems, Networking, and Cybersecurity (SNC) Committee, *Virginia Tech*, 2017-2018
- Faculty Judge for VTURCS Research Symposium, *Virginia Tech*, 2017

# PROFESSIONAL TRAINING

- The Collins Scholars Program, UIUC (2019-2021)

# ADVISING

I am the primary research advisor of the following students:

## Ph.D. Students

- Nicholas Wang (2023 – Present)
  - *CHI '24, WWW '22, Mozilla Bug Bounty*
- Apurva Virkud (2022 – Present, Co-advised with Adam Bates)
  - *USENIX Security '23, USENIX Security '22*
- Hadjer Benkraouda (2021 – Present)
  - *CCS '22 and CCS'23 Student Travel Grant, CCS '23 iMentor*
  - *CHI '24, IEEE SP '23, USENIX Sec '21, AsiaCCS '20, VTS' 20*
- Margie Ruffin (2020 – Present, Co-advised with Kirill Levchenko)
  - *NSF Graduate Research Fellowships Program (GRFP) Award*
  - *Alfred P. Sloan Scholar; Grainger College of Engineering SURGE Fellowship; UIUC Graduate College Fellowship; CCS '20 iMentor*
  - *ICWSM '24, GROUP '23, WPES '22,*
- Zhi Chen (2020 – Present)
  - *IEEE SP '23, DLSP '23, CCS '19*
- Jaron Maurice Mink (2019 – Present)
  - *NSF Graduate Research Fellowships Program (GRFP) Award.*
  - *CHI '24, USENIX Sec'23, IEEE SP '23 (a), IEEE SP '23 (b), IEEE SP '22, USENIX Security '22, CHI '22, WWW '22, ACSAC '20*
- Qingying Hao (2018 – Present)
  - *USENIX Security '23, CCS '21, USENIX Security '21a, IEEE SP '20*
- Limin Yang (2018 – 2023) → ByteDance
  - *IEEE SP Student PC (2021), IBM visiting scholar (2022)*
  - *IEEE SP '23 (a), IEEE SP '23 (b), DLSP '23, USENIX Security '21a, USENIX Security '20, IMC '19, USENIX Security '18b.*
  - *Dissertation: "Machine Learning for Security Applications Under Dynamic and Adversarial Environments"*
- Steve T.K. Jan (2014 – 2020; on leave in 2015) → ByteDance
  - *Intel Fellow Employee Recognition Reward '18, IEEE SP '21 Student Travel Grant*
  - *CCS' 21, USENIX Security'21b, IEEE SP'20, AAAI '19, IMC'18, CIKM '17, SDM '17, SDM '16*
  - *Dissertation: "Robustifying Machine Learning based Security Applications"*
- Hang Hu (2016 – 2020) → Google.
  - *USENIX Security '18 Student Travel Grant*
  - *USENIX Security '21b, IMWUT '20, WWW '20, AsiaCCS '19, IEEE SP '19, IMC '18, USENIX Security '18a, USENIX Security '18b*
  - *Dissertation: "Characterizing and Detecting Online Deception via Data-Driven Methods"*

## Masters Students

- Anusha Ghosh (2023 – Present)
- Nirav Diwan (2022 – Present)
- Zhenning Zhang (2022 – Present)
- Nicholas Wang (2021 – 2023) → PhD at UIUC
  - *Thesis: "VeriSMS: A Message Verification System for Inclusive and Trusted Patient Outreach"*
- Licheng Luo (2020 – 2022) → Jump Trading.
  - *Thesis: "Surveying Face Liveness Detection in the Deepfake Era"*
- Rishabh Chhabra (2020 – 2021) → Amazon.
  - *Thesis: "Empirically Understanding the Global Impact of Migration to DNS-over-HTTPS"*
- Tianrui Hu (2018 – 2020) → PhD at Northeastern.
  - *Thesis: "Detecting Bots using Stream-based System with Data Synthesis"*

- Chao Xu (2018 – 2020) → ByteDance.
  - *Thesis: "Defending Against GPS Spoofing by Analyzing Visual Cues"*
- Jiamin Wang (2018 – 2020) → TSMC → Amazon.
  - *Thesis: "Measuring the Functionality of Amazon Alexa and Google Home Applications"*
- Peng Peng (2017 – 2019) → Palo Alto Networks.
  - *Thesis: "A Measurement Approach to Understanding the Data Flow of Phishing from Attacker and Defender Perspectives"*
- Xiangwen Wang (2017 – 2019) → Google.
  - *Thesis: "Empirical Analysis of User Passwords across Online Services"*
- Chun Wang (2016 – 2018) → IBM.
  - *Thesis: "Photo-based Vendor Re-identification on Darknet Marketplaces using Deep Neural Networks"*

### Undergraduate Students

- Jeffrey Zhai (2023 – Present)
- Shuo Wang (2023 – Present)
- Mutma Adebayo (2022 – Present)
- Sushruth Booma (2022 – Present)
- Ezra Goodwin (2023 – 2024)
- Zhuofan Jia (2022 – Present) → PhD at Duke
- Kevin Tu (2021 – 2022) → Undergrad at UIUC
- JT Kirages (2021 – 2022) → MCS at UIUC
- Saidivya Ashok (2020 – 2021) → MS at CMU *(UIUC Senior Award)*
- Nicholas Wang (2020 – Present) → MS at UIUC
- Olivia Figueira (2020 – 2021) → PhD at UC Irvine
- Zhengdai Hu (2020 – 2021) → Google
- Shihan Lin (2018 – 2019) → PhD at Duke University
- Shinan Liu (2017 – 2019) → PhD at Univ. of Chicago
- Luke Quinn (2018 – 2019) → MITRE
- Douglas Bossart (2017 – 2019) → U.S. Army ERDC

### High School Students

- Megan McQueen (2015) → Yale Undergraduate
- Emily Pan (2015) → Caltech Undergraduate
- Emily Pan (2015) → Caltech Undergraduate

### Visiting Scholars

- Chuhan Wang (2024), PhD at Tsinghua University
- Ying Yuan (2023), PhD at University of Padova→ Postdoc at CISPA

I have served on the program of study committee, qual committee, and thesis committee of the following students:

### Thesis Committee at UIUC (PhD Students)

- **[Current]** Tanusree Sharma; Paul Murley; Kyo Hyun Kim; Tzu-Bin Yan; Yaman Yu; Jingyu Qian; Fan Wu
- **[Graduated in 2023]** Maxwell Bland; Jinhui Song.
- **[Graduated in 2022]** Key-whan Chung; Dongxin Liu.
- **[Graduated in 2021]** Natã Barbosa; Zane Ma; Dominic Seyler.
- **[Graduated in 2020]** Deepak Kumar.

### Program of Study Committee at UIUC (PhD Students)

- **[2022]** Apurva Virkud; Jason Vega; Yao Xiao; Cruz Barnum
- **[2021]** Yuzheng Hu; Sachin Ashok.
- **[2020]** Margie Ruffin; Jinning Li; Muhammad Adil Inam; Nishant Kumar; James Hulett; Zhi Chen.
- **[2019]** Bland, Maxwell; Tzu-Bin Yan; Lecheng Zheng; Akul Goyal; Riccardo Paccagnella; Beitong Tian; Sushant Dinesh.

### Qualification Committee at UIUC (PhD Students)

- **[2023]** Harjasleen Malvai
- **[2022]** Jude Battista (Qual Chair); Muhammad Adil Inam; Nishant Kumar.
- **[2021]** Akul Goyal (Qual Chair); Beitong Tian; Ruta Jawale; Sourav Das.

- **[2020]** Linyi Li (Qual Chair); Kyo Hyun Kim; Richard C Barber; Chaitra Niddodi.

## Thesis Committee at Virginia Tech (PhD and MS Students)

- **[Current]** Xiang Cheng (PhD).
- **[Graduated in 2022]** Stefan Nagy (PhD); Jiameng Pu (PhD).
- **[Graduated in 2021]** Md Salman Ahmed (PhD).
- **[Graduated in 2020]** Tianyi Li (PhD); Arnab Kumar Paul (PhD); Sazzadur Rahaman (PhD); Thomas Lux (PhD).
- **[Graduated in 2019]** Elaheh Raisi (PhD); Divya Ramanujachari (MS); Da Pu (MS); Xinfeng Xu (MS).
- **[Graduated in 2018]** Kexiong Zeng (PhD); Long Cheng (PhD); Nai-Ching Wang (PhD); Alex Hsu (MS); Zachary Burch (MS); Archi Dasgupta (MS).
- **[Graduated in 2017]** Wenhai Sun (PhD); Hannah Roth (MS); Alexander Kedrowitsch (MS); Noah Luther (MS).

## Other External Thesis Committees (PhD Students)

- **[Current]** Faysal Hossain Shezan, UVA
- **[Graduated in 2021]** Duc Cuong Nguyen, CISPA Helmholtz Center for Information Security.