Xiaokuan Zhang

Assistant Professor
George Mason University
4400 University Drive, Fairfax, VA, 22030

Office: Research Hall 357
Email: `xiaokuan@gmu.edu`
Homepage: `https://mainarke.github.io`

Education

Ph.D. in Computer Science and Engineering **The Ohio State University**
Advisor: Prof. Yinqian Zhang Aug. 2015 - Dec. 2021

B.S. in Computer Science and Technology **Shanghai Jiao Tong University**
Advisor: Prof. Haojin Zhu Sep. 2011 - Jun. 2015

Work Experience

Assistant Professor **George Mason University**
Fairfax, VA Aug. 2022 - present

Postdoctoral Researcher **Georgia Institute of Technology**
Atlanta, GA Nov. 2021 - Aug. 2022

Research Intern **Microsoft Research**
Redmond, WA May 2019 - Aug. 2019

Software Engineering Intern **Google Inc.**
Mountain View, CA May 2018 - Aug. 2018

Honors & Awards

• ACM CCS Distinguished Paper Award	2024
• Springer Cybersecurity *Best Practical Research Paper* Award	2024, 2025
• ACM SIGSOFT Distinguished Paper Award	2024
• Ethereum Foundation Academic Round Grant	2023(x2), 2024
• Norton (Symantec) Graduate Fellowship (*three awardees worldwide*)	2020
• Graduate Research Award, CSE Department, Ohio State University	2020
• Nomination for Google Research Fellowship, CSE Department, Ohio State University	2019
• Top 10 Finalists of CSAW Applied Security Research Competition	2016, 2018, 2022
• Outstanding Graduate, Shanghai Jiao Tong University	2015

- Academic Excellence Scholarship, Shanghai Jiao Tong University 2012, 2014
- Outstanding Student Cadre, Shanghai Jiao Tong University 2013

Publications

Summary:
Top-tier security conference papers (20): Oakland x2, CCS x10, USENIX Security x5, NDSS x3
Other top-tier conference papers (7): ASPLOS x1, ATC x1, ICSE x3, Mobicom x1, UIST x1
Top-tier security journals (2): TDSC x2

Peer-reviewed Conferences/Journals/Workshops

1. **[XR-Security'25]** Bertram Liu, Vamsi Shankar Simhadri, **Xiaokuan Zhang**. *"Hunting Insecure UI Properties in Extended Reality"*. In Proceedings of the 26th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc'25), Houston, TX, USA, Oct. 2025. (*workshop paper*)
2. **[CCS'25]** Vamsi Shankar Simhadri, Yichang Xiong, Habiba Farrukh, **Xiaokuan Zhang**. *"Virtual Reality, Real Problems: A Longitudinal Security Analysis of VR Firmware"*. In Proceedings of the 32nd ACM Conference on Computer and Communications Security, Taipei, Oct. 2025.
3. **[AsiaCCS'25]** Kailun Yan, Bo Lu, Pranav Agrawal, Jiasun Li, Wenrui Diao, **Xiaokuan Zhang**. *"An Empirical Study on Cross-chain Transactions: Costs, Inconsistencies, and Activities"*. In Proceedings of the 20th ACM Asia Conference on Computer and Communications Security, Hanoi, Vietnam, Aug. 2025. (*Acceptance rate: 20.4%)*
4. **[Security'25]** Hung-Mao Chen, Xu He, Shu Wang, **Xiaokuan Zhang**, Kun Sun. *"TYPEPULSE: Detecting Type Confusion Bugs in Rust Programs"*. In Proceedings of the 34th USENIX Security Symposium, Seattle, WA, USA, Aug. 2025.
5. **[Oakland'25]** Fan Sang, Jaehyuk Lee, **Xiaokuan Zhang**, Taesoo Kim. *"Portal: Fast and Secure Device Access with Arm CCA for Modern Arm Mobile System-on-Chips (SoCs)"*. In Proceedings of the 46th IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2025. (*Acceptance rate: 14.8%)*
6. **[ICSE'25]** Mengya Zhang, Preksha Shukla, Wuqi Zhang, Zhuo Zhang, Pranav Agrawal, Zhiqiang Lin, Xiangyu Zhang, **Xiaokuan Zhang**. *"An Empirical Study of Proxy Smart Contracts at the Ethereum Ecosystem Scale"*. In Proceedings of the 47th IEEE/ACM International Conference on Software Engineering, Ottawa, Ontario, Canada, Apr. 2025. (*Acceptance rate: 21.3%)*
7. **[ICSE'25]** Xiang Cheng, Fan Sang, Yizhuo Zhai, **Xiaokuan Zhang**, Taesoo Kim. *"RUG: Turbo LLM for Rust Unit Test Generation"*. In Proceedings of the 47th IEEE/ACM International Conference on Software Engineering, Ottawa, Ontario, Canada, Apr. 2025. (*Acceptance rate: 21.3%)*
8. **[FnT-SEC'25]** Kang Li, Ronghui Gu, Jun Xu, Zhaofeng Chen, Siwei Wu, Yajin Zhou, Mu Zhang, Xiapu Luo, Yuzhe Tang, Yi Li, **Xiaokuan Zhang**, Yibo Wang. *"Security Analysis and Formal Verification on Blockchain and its Applications"*. Foundations and Trends® in Privacy and Security. (*journal paper*)
9. **[ACSAC'24]** Mengya Zhang, Xingyu Lyu, Jianyu Niu, **Xiaokuan Zhang**, Yinqian Zhang, Zhiqiang Lin. *"Breaking the Privacy Barrier: On the Feasibility of Reorganization Attacks on Ethereum Private Transactions "*. In Proceedings of the 40th Annual Computer Security Applications Conference,

Waikiki, Hawaii, USA, Dec. 2024. (*Acceptance rate: 19.7%)*

10. **[CCS'24]** Yuxia Zhan, Yan Meng, Lu Zhou, Yichang Xiong, **Xiaokuan Zhang**, Lichuan Ma, Guoxing Chen, Qingqi Pei, Haojin Zhu. *"VPVet: Vetting Privacy Policies of Virtual Reality Apps"*. In Proceedings of the 31st ACM Conference on Computer and Communication Security, Salt Lake City, UT, USA, Oct. 2024. (*Acceptance rate: 16.9%)*

11. **[CCS'24]** Kailun Yan, **Xiaokuan Zhang**, Wenrui Diao. *"Stealing Trust: Unraveling Blind Message Attacks in Web3 Authentication"*. In Proceedings of the 31st ACM Conference on Computer and Communication Security, Salt Lake City, UT, USA, Oct. 2024. (*Acceptance rate: 16.9%)* **ACM CCS Distinguished Paper Award; Springer Cybersecurity Best Practical Research Paper Award**

12. **[CCS'24]** Tong Zhu, Chaofan Shou, Zhen Huang, Guoxing Chen, **Xiaokuan Zhang**, Yan Meng, Shuang Hao, Haojin Zhu. *"Unveiling Collusion-Based Ad Attribution Laundering Fraud: Detection, Analysis, and Security Implications"*. In Proceedings of the 31st ACM Conference on Computer and Communication Security, Salt Lake City, UT, USA, Oct. 2024. (*Acceptance rate: 16.9%)*

13. **[RAID'24]** Mengya Zhang, **Xiaokuan Zhang**, Yinqian Zhang, Zhiqiang Lin. *"Security of Cross-chain Bridges: Attack Surfaces, Defenses, and Open Problems"*. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions, and Defenses, Padua, Italy, Sep. 2024. (*Acceptance rate: 24.4%)*

14. **[Security'24]** Anh Nguyen, **Xiaokuan Zhang**, Zhisheng Yan. *"Penetration Vision through Virtual Reality Headsets: Identifying 360-degree Videos from Head Movements"*. In Proceedings of the 33rd USENIX Security Symposium, Philadelphia, PA, USA, Aug. 2024. (*Acceptance rate: 18.3%)*

15. **[ICSE'24]** Yongliang Chen, Ruoqin Tang, Chaoshun Zuo, **Xiaokuan Zhang**, Lei Xue, Xiapu Luo, Qingchuan Zhao. *"Attention! Your Copied Data is Under Monitoring: A Systematic Study of Clipboard Usage in Android Apps"*. In Proceedings of the 46th IEEE/ACM International Conference on Software Engineering, Lisbon, Portugal, Apr. 2024. (*Acceptance rate: 22.3%)* **ACM SIGSOFT Distinguished Paper Award**

16. **[NDSS'24]** Fan Sang, Jaehyuk Lee, **Xiaokuan Zhang**, Meng Xu, Scott Constable, Yuan Xiao, Michael Steiner, Mona Vij, Taesoo Kim. *"SENSE: Enhancing Microarchitectural Awareness for TEEs via Subscription Based Notification"*. In Proceedings of the 31st Network and Distributed System Security Symposium, San Diego, CA, USA, Feb. 2024. (*Acceptance rate: 15.0%)*

17. **[TDSC'24]** Wei Peng, Xiang Li, Jianyu Niu, **Xiaokuan Zhang**, Yinqian Zhang. *"Ensuring State Continuity for Confidential Computing: A Blockchain-based Approach"*. IEEE Transactions on Dependable and Secure Computing. (*journal paper*)

18. **[CCS'23]** Tao Ni, **Xiaokuan Zhang**, Qingchuan Zhao. *"Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel"*. In Proceedings of the 30th ACM Conference on Computer and Communication Security, Copenhagen, Denmark, Nov. 2023. (*Acceptance rate: 19.2%)* **Springer Cybersecurity Best Practical Research Paper Award**

19. **[Mobicom'23]** Tao Ni, Jianfeng Li, **Xiaokuan Zhang**, Chaoshun Zuo, Wubing Wang, Weitao Xu, Xiapu Luo, Qingchuan Zhao. *"Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning"*. In Proceedings of the 29th Annual International Conference On Mobile Computing And Networking, Madrid, Spain, Oct. 2023. (*Acceptance rate: 24.4%)*

20. **[Security'23]** Lu Zhou, Chengyongxiao Wei, Tong Zhu, Guoxing Chen, **Xiaokuan Zhang**, Suguo Du, Hui Cao, Haojin Zhu. *"POLICYCOMP: Counterpart Comparison of Privacy Policies Uncovers Overbroad Personal Data Collection Practices"*. In Proceedings of the 32nd USENIX Security Symposium, Anaheim, CA, USA, Aug. 2023. (*Acceptance rate: 29.2%)*

21. **[Oakland'23]** Tao Ni, **Xiaokuan Zhang**, Chaoshun Zuo, Jianfeng Li, Zhenyu Yan, Wubing Wang, Weitao Xu, Xiapu Luo, Qingchuan Zhao. *"Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels"*. In Proceedings of the 44th IEEE Symposium on Security and Privacy, San Francisco, CA, USA, May 2023. (*Acceptance rate: 17.0%)*

22. **[ASPLOS'23]** Adil Ahmad, Botong Ou, Congyu Liu, **Xiaokuan Zhang**, Pedro Fonseca. *"Veil: A Protected Services Framework for Confidential Virtual Machines"*. In Proceedings of the 2023 ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Vancouver, Canada, Apr. 2023. (*Acceptance rate: 25.1%)*

23. **[TDSC'23] Xiaokuan Zhang**, Yang Zhang, Yinqian Zhang. *"VERITRAIN: Validating MLaaS Training Efforts via Anomaly Detection"*. IEEE Transactions on Dependable and Secure Computing. (*journal paper*)

24. **[CCS'22]** Jianyu Niu, Wei Peng, **Xiaokuan Zhang**, Yinqian Zhang. *"Narrator: Secure and Practical State Continuity for Trusted Execution on Cloud"*. In Proceedings of the 29th ACM Conference on Computer and Communication Security, Los Angeles, CA, USA, Nov. 2022. (*Acceptance rate: 22.5%)*

25. **[ATC'22]** Fan Sang, Ming-Wei Shih, Sangho Lee, **Xiaokuan Zhang**, Michael Steiner, Mona Vij, Taesoo Kim. *"PRIDWEN: Universally Hardening SGX Programs via Load-Time Synthesis"*. In Proceedings of the 2022 USENIX Annual Technical Conference, Carlsbad, CA, USA, Jul. 2022. (*Acceptance rate: 16.3%)*

26. **[IJIS'22] Xiaokuan Zhang**, Jihun Hamm, Michael K. Reiter, Yinqian Zhang. *"Defeating traffic analysis via differential privacy: a case study on streaming traffic"*. International Journal of Information Security. (*journal paper)*

27. **[CCS'21]** Suibin Sun, Le Yu, **Xiaokuan Zhang**, Minhui Xue, Ren Zhou, Haojin Zhu, Shuang Hao, Xiaodong Lin. *"Understanding and Detecting Mobile Ad Fraud Through the Lens of Invalid Traffic"*. In Proceedings of the 28th ACM Conference on Computer and Communication Security, Virtual Event, Nov. 2021. (*Acceptance rate: 22.3%)* **(Top 10 Finalists of CSAW'22 Applied Security Research Competition)**

28. **[CCS'21]** Tong Zhu, Yan Meng, Haotian Hu, **Xiaokuan Zhang**, Minhui Xue, Haojin Zhu. *"Dissecting Click Fraud Autonomy in the Wild"*. In Proceedings of the 28th ACM Conference on Computer and Communication Security, Virtual Event, Nov. 2021. (*Acceptance rate: 22.3%)*

29. **[UIST'20]** Frederik Brudy, David Ledo, Michel Pahud, Nathalie Henry Riche, Christian Holz, Anand Waghmare, Hemant Surale, Marcus Peinado, **Xiaokuan Zhang**, Shannon Joyner, Badrish Chandramouli, Umar Farooq Minhas, Jonathan Goldstein, Bill Buxton, Ken Hinckley. *"SurfaceFleet: Exploring Distributed Interactions Unbounded from Device, Application, User, and Time"*. In Proceedings of the 33rd Annual Symposium on User Interface Software and Technology, Virtual Event, Oct. 2020. *(Acceptance rate: 21.5%)*

30. **[Security'20]** Mengya Zhang*, **Xiaokuan Zhang***, Yinqian Zhang, Zhiqiang Lin. *"TXSPECTOR: Uncovering Attacks in Ethereum from Transactions"*. In Proceedings of the 29th USENIX Security Sym-

posium, Virtual Event, Aug. 2020. (*Acceptance rate: 16.1%)* (*equal contribution)

31. **[NDSS'19] Xiaokuan Zhang**, Jihun Hamm, Michael K. Reiter, Yinqian Zhang. *"Statistical Privacy for Streaming Traffic"*. In Proceedings of the 26th Network and Distributed System Security Symposium, San Diego, CA, USA, Feb. 2019. (*Acceptance rate: 17.1%)*

32. **[ACSAC'18]** Bo Lu*, **Xiaokuan Zhang***, Ziman Ling, Yinqian Zhang, Zhiqiang Lin. *"A Measurement Study of Authentication Rate-Limiting Mechanisms of Modern Websites"*. In Proceedings of the 34th Annual Computer Security Applications Conference, San Juan, Puerto Rico, USA, Dec. 2018. (*Acceptance rate: 20.1%)* (*equal contribution)

33. **[CCS'18]** Wei Zhang, Yan Meng, Yugeng Liu, **Xiaokuan Zhang**, Yinqian Zhang, Haojin Zhu. *"HoMonit: Monitoring Smart Home Apps from Encrypted Traffic"*. In Proceedings of the 25th ACM Conference on Computer and Communication Security, Toronto, Canada, Oct. 2018. (*Acceptance rate: 16.6%)*

34. **[NDSS'18] Xiaokuan Zhang**, Xueqiang Wang, Xiaolong Bai, Yinqian Zhang, XiaoFeng Wang. *"OS-level Side Channels without Procfs: Exploring Cross-App Information Leakage on iOS"*. In Proceedings of the 25th Network and Distributed System Security Symposium, San Diego, CA, USA, Feb. 2018. (*Acceptance rate: 21.5%)* **(Top 10 Finalists of CSAW'18 Applied Security Research Competition)**

35. **[AsiaCCS'17]** Sanchuan Chen, **Xiaokuan Zhang**, Michael K. Reiter, Yinqian Zhang. *"Detecting Privileged Side-Channel Attacks in Shielded Execution with DEJA VU"*. In Proceedings of the 12th ACM Asia Conference on Computer and Communications Security, Abu Dhabi, UAE, Apr. 2017. (*Acceptance rate: 20.3%)*

36. **[CCS'16] Xiaokuan Zhang**, Yuan Xiao, Yinqian Zhang. *"Return-Oriented Flush-Reload Side Channels on ARM and Their Implications for Android Devices"*. In Proceedings of the 23rd ACM Conference on Computer and Communication Security, Vienna, Austria, Oct. 2016. (*Acceptance rate: 16.5%)*

37. **[Security'16]** Yuan Xiao, **Xiaokuan Zhang**, Yinqian Zhang, Mircea-Radu Teodorescu. *"One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation"*. In Proceedings of the 25th USENIX Security Symposium, Austin, TX, USA, Aug. 2016. (*Acceptance rate: 15.6%)* **(Top 10 Finalists of CSAW'16 Applied Security Research Competition)**

38. **[ICCC'15]** Bett Ben Chirchir, **Xiaokuan Zhang**, Mengyuan Li, Qiyang Qian, Na Ruan, Haojin Zhu. *"SmartSec: Secret Sharing-based Location-aware Privacy Enhancement in Smart Devices".* In Proceedings of the 4th IEEE/CIC International Conference on Communications in China, Shenzhen, China, Nov. 2015.

39. **[GLOBECOM'14] Xiaokuan Zhang**, Haizhong Zheng, Xiaolong Li, Suguo Du, and Haojin Zhu. *"You are Where You Have Been: Sybil Detection via Geo-location Analysis in OSNs".* In Proceedings of the 33rd Global Communications Conference, Austin, TX, USA, Dec. 2014.

Preprints

1. **[Arxiv'22]** Xingyu Lyu, Mengya Zhang, **Xiaokuan Zhang**, Jianyu Niu, Yinqian Zhang, Zhiqiang Lin. *"An Empirical Study on Ethereum Private Transactions and the Security Implications".* arXiv preprint, arXiv:2208.02858.

2. **[Arxiv'21]** Jungwon Lim, Yonghwi Jin, Mansour Alharthi, **Xiaokuan Zhang**, Jinho Jung, Rajat Gupta, Kuilin Li, Daehee Jang, Taesoo Kim. *"SoK: On the Analysis of Web Browser Security".* arXiv preprint, arXiv:2112.15561.

Teaching Experience

Instructor	**George Mason University**
○ CS 795: Security Issues in Emerging Computer and AI Systems	Fall 2025
○ CS 499: Foundations and Advances of Cybersecurity	Fall 2024
○ CS 692: Linux Kernel Internals	Spring 2024, Spring 2025
○ CS 795: Security Issues in Emerging Computer Systems	Fall 2023
○ CS 471: Operating Systems	Fall 2022, Spring 2023

Graduate Teaching Assistant	**The Ohio State University**
○ CSE 3341: Principles of Programming Languages	Spring 2016
○ CSE 3461: Computer Networking and Internet Technologies	Fall 2015

External Service

Organizing Committee

○ Local Chair, ACSIC Symposium on Frontiers in Computing (SOFC)	2025
○ Session Chair, ACM Conference on Computer and Communications Security (CCS)	2024
○ Web Chair, Information Security Conference (ISC)	2024

Program Committee

Conference:

○ ISOC Network and Distributed System Security Symposium (NDSS)	2025, 2026
○ USENIX Security Symposium (Security)	2024, 2025, 2026
○ Annual Computer Security Applications Conference (ACSAC)	2024, 2025
○ ACM Asia Conference on Computer and Communications Security (AsiaCCS)	2024, 2025
○ ACM Conference on Computer and Communications Security (CCS)	2024
○ IEEE Global Blockchain Conference (GBC)	2024
○ International Conference on Mobile Ad-Hoc and Smart Systems (MASS)	2024
○ International Conf. on Applied Cryptography and Network Security (ACNS)	2023
○ EAI International Conf. on Security and Privacy in Comm. Net. (SecureComm)	2022, 2023
○ IEEE International Conf. on Cloud Computing Technology and Science (CloudCom)	2020, 2023
○ International Conf. on Knowledge Science, Engineering and Management (KSEM)	2022

Workshop:

○ Trust-XR Workshop (co-located with ISMAR 2025)	2025

- ○ XR-Security Workshop (co-located with MobiHoc 2025) 2025
- ○ ACM Cloud Computing Security Workshop (CCSW) 2020, 2021, 2022
- ○ NYU CSAW Cyber Security Applied Research Paper Competition 2020, 2021

Journal Reviewer

- ○ IEEE Transactions on Mobile Computing (TMC) 2021, 2022
- ○ IEEE Transactions on Dependable and Secure Computing (TDSC) 2019, 2022 - 2025

External Reviewer

- ○ IEEE Symposium on Security and Privacy (Oakland) 2016 - 2018, 2020, 2022
- ○ ACM Conference on Computer and Communications Security (CCS) 2016 - 2020
- ○ USENIX Security Symposium (Security) 2017, 2022
- ○ ISOC Network and Distributed System Security Symposium (NDSS) 2018, 2020
- ○ ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2018, 2020

Panelist

- ○ National Science Foundation (NSF) 2025

Presentations & Talks

- Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels
  University of Idaho, Virtual (invited) Nov. 2024

- Security and Privacy of Emerging Computer Systems
  Gen Next Education master class (GMU-CS representative), Virtual Nov. 2024

- Beyond the Headset: Unmasking Privacy Challenges in Extended Reality
  NIST Extended Reality (XR) Community of Interest (COI) monthly meeting, Virtual Aug. 2024

- Security and Privacy Issues in the Era of Web3 and Metaverse
  DMV Security Workshop, University of Virginia, Charlottesville, VA, USA Mar. 2024

- POLICYCOMP: Counterpart Comparison of Privacy Policies Uncovers Overbroad Personal Data Collection Practices
  USENIX Security'23, Anaheim, CA, USA Aug. 2023

- Security and Privacy Concerns in Computer Systems – Exploring the Human Connection
  CAHMP Center Mini Symposium, GMU, Fairfax, VA, USA Apr. 2023

- Research Overview – System Security
  Computer Science Research Mixer, GMU, Fairfax, VA, USA Nov. 2022

- Understanding and Detecting Mobile Ad Fraud Through the Lens of Invalid Traffic
  CSAW'22 Applied Security Research Competition, NYU, New York City, NY, USA Nov. 2022

- Side-channel Threats on Modern Platforms
  Stevens Institute of Technology, Virtual Mar. 2021

Penn State University, Virtual Feb. 2021
New Jersey Institute of Technology, Virtual Feb. 2021
Rochester Institute of Technology, Virtual Feb. 2021
George Mason University, Virtual Feb. 2021

- Statistical Privacy for Streaming Traffic
  NDSS'19, San Diego, CA, USA Feb. 2019

- A Measurement Study of Authentication Rate-Limiting Mechanisms of Modern Websites
  ACSAC'18, San Juan, PR, USA Dec. 2018

- OS-level Side Channels without Procfs: Exploring Cross-App Information Leakage on iOS
  CSAW'18 Applied Security Research Competition, NYU, New York City, NY, USA Nov. 2018
  NDSS'18, San Diego, CA, USA Feb. 2018

- Return-Oriented Flush-Reload Side Channels on ARM and Their Implications for Android Devices
  CCS'16, Vienna, Austria Oct. 2016

- You are Where You Have Been: Sybil Detection via Geo-location Analysis in OSNs
  GLOBECOM'14, Austin, TX, USA Dec. 2014