Xiaokuan Zhang

Research Interests

System Security, Side Channels, Privacy

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 — Sep. 2021 - present

Research Intern — **Microsoft Research**

Redmond, WA — May 2019 - Aug. 2019

Software Engineering Intern — **Google Inc.**

Mountain View, CA — May 2018 - Aug. 2018

Honors & Awards

- **NortonLifeLock (Symantec) Graduate Fellowship** 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
- **Outstanding Graduate, Shanghai Jiao Tong University** 2015
- **Academic Excellence Scholarship, Shanghai Jiao Tong University** 2012, 2014
- **Outstanding Student Cadre, Shanghai Jiao Tong University** 2013
- **National Olympiad in Informatics in Provinces (NOIP), First Prize in Fujian Province** 2010

Publications

1. **[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%)*

2. **[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)*

3. **[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%)*

4. **[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%)*

5. **[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%)*

6. **[Security'20]** Mengya Zhang*, **Xiaokuan Zhang***, Yinqian Zhang, Zhiqiang Lin. *"TXSPECTOR: Uncovering Attacks in Ethereum from Transactions"*. In Proceedings of the 29th USENIX Security Symposium, Virtual Event, Aug. 2020. (*Acceptance rate: 16.1%)* (*equal contribution)

7. **[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%)*

8. **[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)

9. **[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%)*

10. **[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)**

11. **[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%)*

12. **[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%)*

13. **[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)**
14. **[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, Senzhen, China, Nov. 2015.
15. **[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.

Teaching Experience

Graduate Teaching Assistant **The Ohio State University**

- CSE 3341: Principles of Programming Languages Jan. 2016 - May 2016
- CSE 3461: Computer Networking and Internet Technologies Aug. 2015 - Dec. 2015

Undergraduate Teaching Assistant **Shanghai Jiao Tong University**

- EI 209: Computer Architecture and Design Sep. 2014 - Jan. 2015

Service

Program Committee

- International Conf. on Applied Cryptography and Network Security (ACNS) 2023
- EAI International Conf. on Security and Privacy in Comm. Net. (SecureComm) 2022
- International Conf. on Knowledge Science, Engineering and Management (KSEM) 2022
- ACM Cloud Computing Security Workshop (CCSW) 2020, 2021
- NYU CSAW Cyber Security Applied Research Paper Competition 2020, 2021
- IEEE International Conf. on Cloud Computing Technology and Science (CloudCom) 2020

Journal Reviewer

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

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

Presentations & Talks

- 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, 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

References

Yinqian Zhang, Professor
Southern University of Science and Technology
yinqianz@acm.org

Zhiqiang Lin, Professor
The Ohio State University
zlin@cse.ohio-state.edu

Michael K. Reiter, Professor
Duke University
michael.reiter@duke.edu

Taesoo Kim, Professor
Georgia Institute of Technology
taesoo@gatech.edu