Fan Sang

Ph.D. in Computer Science9F South, CODA Building756 W Peachtree St NW, Atlanta, GA 30308

Research Interests

I am interested in all areas of **system security and privacy**, with an emphasis on confidential computing, side-channel security, edge and IoT security, and reverse engineering.

EDUCATION

- Georgia Institute of Technology (GaTech), Atlanta, GA Ph.D. in Computer Science; Advisor: Professor Taesoo Kim
- University of Southern California (USC), Los Angeles, CA B.S. in Computer Science; Graduated magna cum laude

PUBLICATIONS

- [1] [NDSS'24] Fan Sang, Jaehyuk Lee, Xiaokuan Zhang, Meng Xu, Scott Constable, Yuan Xiao, Michael Steiner, Mona Vij, and Taesoo Kim. "Sense: Enhancing Microarchitectural Awareness for TEEs via Subscription-Based Notification". In Proceedings of the 2024 Annual Network and Distributed System Security Symposium, Feb 2024, San Diego, CA (acceptance rate: 15.0% = 104/694) [PDF]
- [2] [ATC'22] Fan Sang, Ming-Wei Shih, Sangho Lee, Xiaokuan Zhang, Michael Steiner, Mona Vij, and Taesoo Kim. "Pridwen: Universally Hardening SGX Programs via Load-Time Synthesis". In Proceedings of the 2022 USENIX Annual Technical Conference, Jul 2022, Carlsbad, CA (acceptance rate: 16.2% = 64/394) [PDF]
- [3] [CCS'21] Ren Ding, Yonghae Kim, Fan Sang, Wen Xu, Gururaj Saileshwar, and Taesoo Kim. "Hardware Support to Improve Fuzzing Performance and Precision". In Proceedings of the 28th ACM Conference on Computer and Communications Security, Nov 2021, Seoul, South Korea (acceptance rate: 22.3% = 196/879) [PDF]

PREPRINTS AND OTHERS

- [1] Author of **SGX101**: *https://sgx101.gitbook.io/sgx101/* (sponsored by Intel), an Intel SGX tutorial website with programming examples and reference resources. [Github][Sample]
- [2] Jaehyuk Lee, **Fan Sang**, and Taesoo Kim. "Prime+Retouch: When Cache is Locked and Leaked". arXiv:2402.15425 [cs.CR], Feb 2024 [PDF]
- [3] Xin Jin, Charalampos Katsis, Fan Sang, Jiahao Sun, Elisa Bertino, Ramana Rao Kompella, and Ashish Kundu. "Graphene: Infrastructure Security Posture Analysis with AI-generated Attack Graphs". arXiv:2312.13119 [cs.CR], Dec 2023 [PDF]
- [4] Xin Jin, Charalampos Katsis, Fan Sang, Jiahao Sun, Ashish Kundu, and Ramana Kompella. "Edge Security: Challenges and Issues". arXiv:2206.07164v1 [cs.CR], Jun 2022 [PDF]
- [5] Fan Sang, Daehee Jang, Ming-Wei Shih, and Taesoo Kim. "P²FaaS: Toward Privacy-Preserving Fuzzing as a Service". arXiv:1909.11164 [cs.CR], Sep 2019 [PDF]

(310) 307-9797 fsang@gatech.edu https://sang.fan/

Jun 2018 - Jul 2024

Aug 2014 - May 2018

PATENTS

[1] Junbum Shin, Fan Sang, Meng Xu, and Taesoo Kim, Access point and communication connection method therefor, US20220345890A1.

Delivered Research Proposals

- Title: Enabling Rack-Scale Disaggregation-Aware Confidential Computing via Intel IPUs 2024 Agency/Company: Intel Total Dollar Amount: \$420,000/3 years
- Title: EdgeShield: Defeating Next-generation Cyber Threats on the Edge Environment 2022 Agency/Company: Cisco Total Dollar Amount: \$154,000/year
- Title: SGX101: Example-based, Security-focused Educational Modules for Learning SGX 2019 Agency/Company: Intel Total Dollar Amount: \$15,000/year

WORK EXPERIENCE

• Research Assistant, Georgia Institute of Technology, Atlanta, GA System and security research in System Software & Security Lab. Advisor: Professor Taesoo Kim	Jun 2018 - Jul 2024
• Security Research Internship, Cisco, San Jose, CA Holistic security of edge computing. Supervisor: Dr. Ashish Kundu	May 2022 - Aug 2022
• Security Research Internship, ByteDance, Mountain View, CA Rust implementation of Intel SGX Provisioning Certificate Caching Service (PCCS). A Design of Rust PCCS with Certificate Transparency. Supervisor: Dr. Yu Ding	May 2020 - Aug 2020
• Security Research Internship, Baidu X-Lab, Sunnyvale, CA Abnormal account activities detection using neural network. Supervisor: Dr. Tao Wei	Jun 2017 - Aug 2017
TEACHING EXPERIENCE	
• Teaching Assistant, Georgia institute of Technology, Atlanta, GA Teaching Assistant for CS 6265, Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2021/).	Aug 2021 - Dec 2021
• Teaching Assistant, Georgia institute of Technology, Atlanta, GA Teaching Assistant for CS 6265, Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2020-spring).	Jan 2020 - May 2020
• Teaching Assistant, Georgia institute of Technology, Atlanta, GA Teaching Assistant for CS 6265, Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2019/).	Aug 2019 - Dec 2019
• Teaching Assistant, University of Southern California, Los Angeles, CA Teaching Assistant for CSCI 270, Introduction to Algorithms and Theory of Computing.	Aug 2017 - May 2018
• Teaching Assistant, University of Southern California, Los Angeles, CA Teaching Assistant for CSCI 103, Introduction to Programming.	Aug 2016 - Dec 2016

Service

• Program Committee	
EAI International Conference on Security and Privacy in Communication Networks (SecureComm)	2024
European Conference on Computer Systems (EuroSys) Shadow PC	2024
USENIX Security Symposium (Security) Artifact Evaluation	2024
NYU CSAW Cyber Security Applied Research Paper Competition	2023
• Reviewer	
ACM Transactions on Privacy and Security (TOPS)	2024
IEEE International Conference on Data Engineering (ICDE)	2024
IEEE International Conference on Cloud Computing Technology and Science (CloudCom)	2023
IEEE International Conference on Mobility, Sensing and Networking (MSN)	2023
ACM Cloud Computing Security Workshop (CCSW)	2023
EAI International Conference on Security and Privacy in Communication Networks (SecureComm)	2023
IEEE Transactions on Computers (TC)	2022
IEEE Transactions on Dependable and Secure Computing (TDSC)	2022
• External Reviewer	
USENIX Security Symposium (Security)	2024
ACM Conference on Computer and Communications Security (CCS)	2019, 2024
ACM Asia Conference on Computer and Communications Security (AsiaCCS)	2023
IEEE Symposium on Security and Privacy (Oakland)	2019, 2022
ISOC Network and Distributed System Security Symposium (NDSS)	2020
ACM Symposium on Operating Systems Principles (SOSP)	2021
USENIX Annual Technical Conference (ATC)	2019
USENIX Symposium on Networked Systems Design and Implementation (NDSI)	2020
Presentations & Talks	
• Sense: Enhancing Microarchitectural Awareness for TEEs via Subscription-Based	Notification
NDSS, San Diego, CA	Feb 2024
• Pridwen: Universally Hardening SGX Programs via Load-Time Synthesis USENIX ATC, Carlsbad, CA	Jul 2022
- Creation of Helictic Educ Security Destance Monogenerat (Demo)	
• Graphene: Honstic Edge Security Posture Management (Demo)	Lup 2022
ACM SIGMETRICS/IFIP PERFORMANCE, VIITUAI	Juli 2022
OPEN SOURCE CONTRIBUTIONS	
• SGX101: an example-based, security-focused educational modules for learning SGX. https://github.com/sslab-gatech/sgx101-gitbook	
nttps://gitnub.com/sangiansn/SGA101_sample_code	
• Pridwen: a framework that selectively applies SCA countermeasures for SGX programs. https://github.com/sslab-gatech/Pridwen	
• Sense: a solution that directly exposes microarchitectural events to userspace TEEs. https://github.com/sslab-gatech/Sense	
• SNAP: a customized hardware platform to enhance coverage-guided fuzzing. https://github.com/sslab-gatech/SNAP	
Awards and Activities	
• DEFCON 27 CTF, 8th place (r00timentary), Las Vegas, NV	Aug 2019
• Magna cum Laude, Graduation with University Honors, USC	May 2018

• Academic Achievement Awards and Deans List, USC

Aug 2014 - May 2018

Programming Languages: C, C++, Rust, Python, Java **Technologies:** VR/AR/XR, side channels, Intel SGX, IoT, wireless network, fuzzing test, AWS

References

Taesoo Kim (advisor), Professor Georgia institute of Technology taesoo@gatech.edu

Xiaokuan Zhang, Assistant Professor George Mason University xiaokuan@gmu.edu Ashish Kundu, Head of Cybersecurity Research Cisco Research ashkundu@cisco.com

Meng Xu, Assistant Professor University of Waterloo meng.xu.cs@uwaterloo.ca