Fan Sang

Ph.D. Candidate
9F South, CODA Building
756 W Peachtree St NW, Atlanta, GA 30308

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

Research Interests

I am interested in areas of **system security and privacy**, including trusted computing, side-channel security, edge and IoT security, and reverse engineering. Currently I am exploring the interdisciplinarity of **trusted computing and XR security**.

Education

- **Georgia Institute of Technology (GaTech)**, Atlanta, GA — Jun 2018 - Jul 2024 (expected)
  Ph.D. in Computer Science; Advisor: Professor Taesoo Kim
- **University of Southern California (USC)**, Los Angeles, CA — Aug 2014 - May 2018
  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. "Prometheus: 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. "P^{2}FaaS: Toward Privacy-Preserving Fuzzing as a Service".
arXiv:1909.11164 [cs.CR], Sep 2019 [PDF]

Patents

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

Grants and Funding

- **Cisco Research Funding ($154k)** 2022
  Delivered proposal on defeating next-generation cyber threats in the edge environment.
  Resulted in $154k research funding from Cisco.

Work Experience

- **Research Assistant**, **Georgia Institute of Technology**, Atlanta, GA Jun 2018 - Present
  System and security research in *System Software & Security Lab.*
  Advisor: Professor Taesoo Kim
- **Security Research Internship**, **Cisco**, San Jose, CA May 2022 - Aug 2022
  Holistic security of edge computing.
  Supervisor: Dr. Ashish Kundu
- **Security Research Internship**, **ByteDance**, Mountain View, CA May 2020 - Aug 2020
  Rust implementation of Intel SGX Provisioning Certificate Caching Service (PCCS).
  A Design of Rust PCCS with Certificate Transparency.
  Supervisor: Dr. Yu Ding
- **Security Research Internship**, **Baidu X-Lab**, Sunnyvale, CA Jun 2017 - Aug 2017
  Abnormal account activities detection using neural network.
  Supervisor: Dr. Tao Wei

Teaching Experience

- **Teaching Assistant**, **Georgia institute of Technology**, Atlanta, GA Aug 2021 - Dec 2021
  Teaching Assistant for CS 6265,
  Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2021/).
- **Teaching Assistant**, **Georgia institute of Technology**, Atlanta, GA Jan 2020 - May 2020
  Teaching Assistant for CS 6265,
  Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2020-spring).
- **Teaching Assistant**, **Georgia institute of Technology**, Atlanta, GA Aug 2019 - Dec 2019
  Teaching Assistant for CS 6265,
  Information Security Labs (CTF) (https://tc.gts3.org/cs6265/2019/).
- **Teaching Assistant**, **University of Southern California**, Los Angeles, CA Aug 2017 - May 2018
  Teaching Assistant for CSCI 270,
  Introduction to Algorithms and Theory of Computing.
- **Teaching Assistant**, **University of Southern California**, Los Angeles, CA Aug 2016 - Dec 2016
  Teaching Assistant for CSCI 103,
  Introduction to Programming.

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 Asia Conference on Computer and Communications Security (AsiaCCS)	2023
IEEE Symposium on Security and Privacy (Oakland)	2019, 2022
ACM Conference on Computer and Communications Security (CCS)	2019
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
- **Graphene: Holistic Edge Security Posture Management (Demo)**
  ACM SIGMETRICS/IFIP PERFORMANCE, Virtual — Jun 2022

Open Source Contributions

- **SGX101:** an example-based, security-focused educational modules for learning SGX.
  https://github.com/sslab-gatech/sgx101-gitbook
  https://github.com/sangfansh/SGX101_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

Technical Strengths

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