

Feng Xiao

SOFTWARE ENGINEER AT GOOGLE

☎(+1) 814-777-7019 | ✉f3ixiao@gmail.com | 🏠fxiao.me | 📧xiaofen9 | 🌐f-xiao

Summary

I am a software engineer at Google. I earned CS Ph.D. from Georgia Tech, where I designed adversarial approaches to improve the privacy and security of machine learning/software systems.

Published 5+ first-author research works at top-tier conferences including IEEE S&P, USENIX SEC, BlackHat USA, etc. Member of Program Committees at premium AI conferences including NeurIPS and ACM WWW.

Work Experience

Google

SOFTWARE ENGINEER

CA, USA

Aug. 2023 - now

- I own image ads on iOS Youtube Shorts.
- **Techniques: Recommendation systems**

Palo Alto Networks

SENIOR STAFF RESEARCHER

CA, USA

Dec. 2023 - Aug. 2024

- Led the research and development of company's first adversarial GenAI product, resulting in 2 approved US patent filings and 1 top-tier academic publication.
- Design the first transformer-based Script Malware detector, contributing 10% detection improvement for previous false negatives.
- Developed and optimized a machine learning feature management infrastructure, reducing data processing overhead from hours to minutes.
- **Techniques: LLM safety, Online learning, Model post-training**

Google

SOFTWARE ENGINEER INTERN

WA, USA

May. 2021 - Aug. 2021

- Designed and implemented the Tsunami Callback Service, which enables Google Cloud Vulnerability Scanner to detect log4j-like vulnerabilities. My work is now open-sourced and actively maintained by Google <https://github.com/google/tsunami-security-scanner-callback-server>
- Leveraged CI/CD techniques in Google to launch my project in production environments (early launch, exceeding expectation).
- Gave two tech talks at Google. I shared my previous research works on web vulnerability analysis.
- **Techniques: Java, Distributed Systems, Low-latency System Design, OWASP Vulnerability Assessment, Kubernetes.**

Google

SOFTWARE ENGINEER INTERN

WA, USA

May. 2020 - Aug. 2020

- Made fundamental changes to the Linux virtual memory management system to enable fast I/O for Confidential VMs at Google Cloud.
- Improved Confidential VM network throughput by 20%.
- Identified a potentially serious bug in our product and received a Google Peer Bonus Award.
- **Techniques: C&C++, Linux Memory Management, Linux I/O Internals, Cloud Virtualization, AMD SEV, Confidential Computing.**

Education

Georgia Institute of Technology

PH.D. IN COMPUTER SCIENCE

Atlanta, USA

Jul. 2019 - Dec. 2023

- GPA: 3.9/4

Wuhan University

B.S. IN COMPUTER SCIENCE

Wuhan, China

Sept. 2014 - Jun. 2018

- GPA: 3.87/4

Publication

5 FIRST-AUTHOR WORKS IN TOP-TIER CONFERENCES

FaceObfuscator: Defending Deep Learning-based Privacy Attacks with Gradient Descent-Resistant Features in Face Recognition.

USENIX SEC'24

SHUAIFAN JIN, HE WANG, ZHIBO WANG, **FENG XIAO**, JIAHUI HU, YUAN HE, WENWEN ZHANG, ZHONGJIE BA, WEIJIE FANG, SHUHONG YUAN, KUI REN

JASMINE: Scale up JavaScript Static Security Analysis with Computation-based Semantic Explanation.

IEEE S&P'24

FENG XIAO, ZHONGFU SU GUANGLIANG YANG, AND WENKE LEE

WEBRR: A Forensic System for Replaying and Investigating Web-Based Attacks in The Modern Web.

USENIX SEC'24

JOEY ALLEN, ZHENG YANG, FENG XIAO, MATTHEW LANDEN, ROBERTO PERDISCI, WENKE LEE

Understanding and Mitigating Remote Code Execution Vulnerabilities in Cross-Platform Ecosystem.

ACM CCS'22

FENG XIAO, IAN ZHENG, JOEY ALLEN, GUANGLIANG YANG, AND WENKE LEE

Abusing Hidden Properties to Attack Node.js Ecosystem.

USENIX Security'21

FENG XIAO, JIANWEI HUANG, YICHANG XIONG, GUANGLIANG YANG, HONG HU, GUOFEI GU, AND WENKE LEE

Discovering Hidden Properties to Attack Node.js Ecosystem.

BlackHat'20

FENG XIAO, JIANWEI HUANG, YICHANG XIONG, GUANGLIANG YANG, HONG HU, GUOFEI GU, AND WENKE LEE

Unexpected Data Dependency Creation and Chaining: A New Attack to SDN.

IEEE S&P'20

FENG XIAO, JINQUAN ZHANG, JIANWEI HUANG, GUOFEI GU, DINGHAO WU, PENG LIU

PatternListener: Cracking Android Pattern Lock Using Acoustic Signals.

ACM CCS'18

MAN ZHOU, QIAN WANG, JINGXIAO YANG, QI LI, FENG XIAO, ZHIBO WANG, XIAOFENG CHEN.

Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller.

DEFCON'18

FENG XIAO, JIANWEI HUANG, PENG LIU.

Enabling Secure Location Authentication in Drone (poster).

ACM MobiCom'17

FENG XIAO, MAN ZHOU, YOUCHENG LIYE, JINGXIAO YANG, QIAN WANG.

Honors

2021	Most Innovative Research Runner-up	Pwnie Award, USA
2019	Chair Fellowship.	Atlanta, USA
2018	Rednor IST Fellowship.	State College, USA
2018	ACM CCS Student Travel Grant Award.	Toronto, Canada
2017	LeiJun Scholarship (Top 1 out of 310).	Wuhan, China
2016	National Scholarship (Awarded to top 0.2% undergrads nationwide)	Wuhan, China
2015	Yuanyi Scholarship.	Wuhan, China

Programming languages

Natively fluent: Java, Python, Node.js

Conversationally fluent: C, PHP, Matlab