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 my CS Ph.D. from Georgia Tech, where I design adversarial cyber-reasoning systems to improve the safety and privacy of software/machine learning systems.

Published 7 research works at top-tier academic conferences (4 first-author ones) such as IEEE S&P and USENIX SEC. Member of Program Committees at premium AI conferences including NeurIPS and ACM WWW.

Work Experience

Google — *CA, USA*

Software Engineer — *Aug. 2024 - now*

- Machine Learning for Youtube Recommendation Systems

Palo Alto Networks — *CA, USA*

Senior Researcher — *Dec. 2023 - Aug, 2024*

- Led the research and development of company's first adversarial GenAI product, resulting in one company-approved US patent filing.
- Lead the development of the transformer encoder-based Script Malware detection, contributing 10% detection improvement for previous false negatives.
- Developed efficient neural n-gram model for on-device filetype identification.
- **Techniques: AI safety, Natural Language Processing, Online learning**

Education

Georgia Institute of Technology — *Atlanta, USA*

Ph.D. in Computer Science — *Jul. 2019 - Dec. 2023*

- Advisor: Dr. Wenke Lee
- Research focus: Systems security, program analysis

Wuhan University — *Wuhan, China*

B.S. in Computer Science — *Sept. 2014 - Jun. 2018*

- Advisor: Dr. Qian Wang, Dr. Zhibo Wang
- GPA: 3.87/4

Publication

4 FIRST-AUTHOR WORKS IN TOP-TIER CONFERENCES

RedAgent: Red Teaming Large Language Models with Context-aware Autonomous Language Agent. — *arxiv*

Huiyu Xu, Wenhui Zhang, Zhibo Wang, **Feng Xiao**,Rui Zheng, Yunhe Feng, Zhongjie Ba, Kui Ren

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