Feng **Xiao**

Machine learning researcher at Palo Alto Networks

(+1) 814-777-7019 | f3ixiao@gmail.com | fxiao.me | xiaofen9 | f-xiao

Summary

I am a machine learning researcher working at Palo Alto Networks. Prior to that, I earned CS Ph.D. from Georgia Tech, where I conducted research in machine learning (ML) and systems security&privacy. 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 ACM WWW.

Education

Georgia Institute of Technology

Atlanta, USA

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

- Worked on Software security and machine learning with Prof. Wenke Lee.
- GPA: 3.9/4

Wuhan University

Wuhan, China

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

- GPA: 3.87/4

Work Experience

Palo Alto Networks

CA, USA

Senior Staff Researcher — *Dec. 2023 - Now*

- Leading the development of Transformer-based representation learning for text-based malware analysis, contributing 10% detection improvement for previous false negatives.
- Developing and optimizing large-scale data pipeline (with BigQuery) for ML feature selection and generation, reducing data processing overhead from hours to minutes.
- Developing algorithms for tracking and explaining concept drifting in ML pipelines, addressing out-of-distribution and adversarial sample challenges.
- **Techniques: Language Models, Online learning, Machine learning model serving, SQL for data processing pipeline**

Google

WA, USA

Software Engineer Intern — *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

WA, USA

Software Engineer Intern — *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.**

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