Feng Xiao

PhD. student In Computer Science

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

Summary

CS Ph.D. student at Georgia Tech. I build automatic software/network protection systems for important Internet Infrastructure (e.g., npm supply chain, Software-defining Network). Discovered 50+ serious vulnerabilities from popular software such as mongodb. 5 research publications at top security conferences (BlackHat USA, Oakland, USENIX SEC, etc). Interested in **cybersecurity system development** and **backend software development**.

Education

Georgia Institute of Technology — *Atlanta, USA*

Ph.D. in Computer Science — *July. 2019 - Now*

- Working on system security 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

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, OWASP vulnerability assessment, Low-latency System Design, Distributed Systems, 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, Cloud Virtualization, AMD SEV, Confidential Computing.**

Penn State University — *State College, USA*

Research Personnel — *Jun. 2018 - May. 2019*

- Proposed SVHunter, a security assessment and vulnerability finding tool for Software-defined networking (SDN) controllers.
- Discovered 18 previously unknown security risks from 4 most widely used SDN controllers using SVHunter, and 9 CVEs were assigned for discovering these vulnerabilities.
- **Techniques: Java, Software-defined Networking (SDN), Network Protocol Design and Implementation, Distributed Systems.**

Tencent — *Shenzhen, China*

Security Engineer Intern — *Aug. 2017 - Sep. 2017*

- Captured and mitigate one 0day attack (CVE 2017-9805) against servers of our company.
- Found 8 high-risk vulnerabilities from the products of Tencent.
- **Techniques: Python, Penetration Testing, Web Security.**

Project Experience

Fortifying Software Supply Chain Infrastructure With Automatic Program Analysis — *Atlanta, USA*

Georgia Tech — *Oct. 2019 - now*

- Designed novel automatic systems (program analysis-based and machine learning-based) to defend/pinpoint vulnerable systems
- Published 4 research papers in top-tier academic conferences
- **Techniques: JavaScript, Program Analysis, Natural Language Processing (NLP), SQL, Software Sandboxing.**

Malware Automatic Analysis and Testing *Atlanta, USA*

Georgia Tech *Jan. 2023 - now*

- Developed an automatic Windows malware analysis pipeline, which involves malware program analysis and malware constrained execution.
- **Techniques: C++, Low-level System Programming, Malware Analysis, Intel Processor Trace, gRPC, K8S.**

Node.js Hidden Property Abusing *Atlanta, USA*

Georgia Tech *Oct. 2019 - Oct. 2020*

- Discovered Hidden Property Abusing (HPA), a novel security risk in Node.js.
- Presented the work at the top industry security conference Blackhat USA. Our work was recognized and followed up by many other research teams and private companies such as JHU SecLab and snyk.
- **Techniques: Node.js, Dynamic Program Tracing.**

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*

Publication

5 FIRST-AUTHOR WORKS IN TOP-TIER CONFERENCES

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

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.

Programming languages

Natively fluent: C, Java, Python, Node.js

Conversationally fluent: C++, PHP, Matlab