

Feng Xiao

| | | |
|---------------------|--|---|
| CONTACT INFORMATION | 756 W Peachtree St NW Atlanta, GA 30308 | feng@gatech.edu www.fxiao.me |
| RESEARCH INTERESTS | Software security, web security, and program analysis. My work has been used by top companies like Google and resulted in many important updates in the popular open source software such as MongoDB (more than 30 CVEs are assigned). | |
| EDUCATION | Georgia Institute of Technology, USA Ph.D. in Computer Sciences | August 2019 - now |
| | Wuhan University, China B.E. in Computer Science | Sept 2014 - June 2018 |
| PUBLICATIONS | 4 papers in top-tier academic security conferences (Okaland, CCS, SEC) 3 papers in top-tier industry security conference (BlackHat USA, DEFCON USA) | |

PEER-REVIEWED CONFERENCES

- [1] *Understanding and Mitigating Remote Code Execution Vulnerabilities in Cross-Platform Ecosystem*
Feng Xiao, Zheng Yang, Joey Allen, Guangliang Yang, Grant Williams, Wenke Lee
In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2022.
- [2] *Abusing Hidden Properties to Attack Node.js Ecosystem*
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee
In Proceedings of the USENIX Security Symposium (SEC), 2021.
- [3] *Active Link Obfuscation to Thwart Link-flooding Attacks for Internet of Things*
Xuyang Ding, **Feng Xiao**, Man Zhou, Zhibo Wang
In Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020.
- [4] *Unexpected Data Dependency Creation and Chaining: A New Attack to SDN*
Feng Xiao, Jinqun Zhang, Jianwei Huang, Guofei Gu, Dinghao Wu, Peng Liu
In Proceedings of the IEEE Symposium on Security and Privacy (Oakland), 2020.
- [5] *PatternListener: Cracking Android Pattern Lock Using Acoustic Signals*
Man Zhou, Qian Wang, Jingxiao Yang, Qi Li, **Feng Xiao**, Zhibo Wang, Xiaofeng Chen
In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2018.
- [6] *CHAOS: An SDN-Based Moving Target Defense System*
Yuan Shi, Huanguo Zhang, Juan Wang, **Feng Xiao**, Jianwei Huang, Daochen Zha
In Proceedings of Security and Communication Networks (SCN), 2017.

INDUSTRIAL CONFERENCE/POSTER

- [7] *Discovering Hidden Properties to Attack the Node.js Ecosystem*
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee
In Black Hat USA Briefings, 2020.
- [8] *Hidden Properties in Node.js Ecosystem*
Feng Xiao, Jianwei Huang, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee
In DEFCON USA Briefings, 2020.

- [9] *Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller*
Feng Xiao, Jianwei Huang, Peng Liu
 In DEFCON USA Briefings, 2018.
- [10] *Enabling Secure Location Authentication in Drone (poster)*
Feng Xiao, Man Zhou, Youchen Liye, Qian Wang
 In the 23th Annual International Conference on Mobile Computing and Networking (MobiCom), 2017

| | | |
|-------------------|--|------|
| HONORS AND AWARDS | Most Innovative Research Award Runner-Up, Pwnie Award | 2020 |
| | Presidential Scholarship (9000 USD), Georgia Tech | 2019 |
| | ACM CCS Student Travel Grant | 2018 |
| | Rednor IST Fellowship (7000 USD), Penn State University | 2018 |
| | Xiaomi Scholarship (3000 USD), Wuhan University | 2017 |
| | ACM MobiCom Student Travel Grant (1000 USD) | 2017 |
| | 🏆 China National Scholarship (Highest student honor nation wide, 1200 USD) | 2016 |
| | Yuanyi Scholarship (3000 USD), Wuhan University | 2015 |
| | Hall of Fame, T00ls (largest Chinese security community) | 2014 |

RESEARCH GRANTS **AI-Assisted Prevention of Supply Chain Attacks on Programming Language Package Mangers**
 Senior Personnel.
 Defense Advanced Research Projects Agency (DARPA)
 With Wenke Lee (co-PI) and Taesoo Kim
 07/2021 - 12/2022

Interactive Editing Techniques for Subsetting and Dialeting Network Protocol
 Senior Personnel.
 Office of Navel Research (ONR)
 With Taesoo Kim (PI), Brendan Saltaformaggio, William Harris, Santosh Pande, Alessandro Orso and Wenek Lee
 04/2018 - 10/2023

OPEN SOURCE CONTRIBUTION **Tsunami-Callback:** An web vulnerability detection service used and maintained by Google
 Lead author.
<https://github.com/google/tsunami-security-scanner-callback-server>

Lynx: An automatic tool for detecting JavaScript hidden property vulnerabilities
 Lead author.
<https://github.com/xiaofen9/XGuard>

SVHunter: An automatic tool for detecting cross-component data poisoning issues in Software-defining Networking (SDN) Controllers
 Lead author.
<https://github.com/xiaofen9/SVhunter>

INVITED TALKS **Automatic Web Vulnerability Detection**
 Google, Virtually 2019

Abusing Hidden Properties to Attack Node.js Ecosystem
 USENIX Security, Virtually 2021

| | |
|-------------------------|------|
| BlackHat USA, Virtually | 2020 |
| DEFCON USA, Virtually | 2020 |

| | |
|--|------|
| Unexpected Data Dependency Creation and Chaining: A New Attack to SDN | |
| Oakland, Virtually | 2020 |

| | |
|--|------|
| Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller | |
| DEFCON USA, Virtually | 2019 |

TEACHING
EXPERIENCE

School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA

| | |
|---|-------------------|
| <i>Graduate Teaching Assistant</i> | August 2022 - now |
| <i>CS 6035 Introduction to Information Security</i> | |