Feng **Xiao**

PhD. student In Computer Science

☎ (+1) 814-777-7019 | ✉ feng@gatech.edu | ⌂ fxiao.me | xiaofen9 | f-xiao

Summary

Second-year PhD. student at Georgia Tech. 8 years experience specializing in the security tool development and OS hacking. Obtained 22 CVEs from widely used software. Experienced in web security, OS driver development, and virtualization security.

Project Experience

Nodejs Program Analysis and Automatic Bug Finding

Atlanta, USA

Georgia Tech — *Oct. 2019 - Now*

- Discovered Hidden Property Abusing (HPA), a new security issue in Node.js ecosystem.
- Built Lynx, an Nodejs bug finding and exploiting tool by combining dynamic data flow tracking, static syntax analysis and symbolic execution (`https://github.com/xiaofen9/Lynx`).
- Identified 15 previously unknown vulnerabilities from 100 widely used nodejs modules (e.g., MongoDB, class-validator).
- The work has been accepted by BlackHat USA 2020.

Windows Kernel Hacking

Wuhan, China

Anonymous Red Team — *Jul. 2017 - Feb. 2018*

- Proposed a new kernel object hijacking method which bypassed the latest Windows Kernel Protection (valid until Feb 2018).
- Developed an ALL-patform Windows rootkit (40+ KLoC C).

Security Assessment on Android App Cryptography

Shanghai, China

Shanghai Jiaotong University — *Jun. 2016 - Aug. 2016*

- Discovered a new universal security risk shared by the majority of mobile apps, which can be exploited to forge apps' cryptographically consistent messages to abuse mobile services.
- Built a dynamic Android cryptography hook framework StupidHam to semi-automatically verified discovered bugs (`https://github.com/xiaofen9/StupidHam`)
- This new discovery honored as the most valuable vulnerability by Wooyun, the biggest bug hunting community in China.

Work Experience

Google

WA, USA

Software Engineer Intern — *May. 2020 - Aug. 2020*

- Made fundamental changes to the Linux virtual memory management system to enable fast and secure I/O for Confidential VMs (CVM).
- Improved CVM network throughput by 20%
- Identified a potential serious performance bug in our product and got awarded a peer bonus.

Penn State University

State College, USA

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

- Proposed SVHunter, a security assessment and vulnerability finding tool for Software-defined networking (SDN) controllers. We open sourced SVHunter at `https://github.com/xiaofen9/SVHunter`.
- Discovered 18 previously unknown security risks from 4 most widely used SDN controllers using SVHunter, and 9 CVEs were assigned for discovering these vulnerabilities.
- The proposed work has been accepted to IEEE S&P'20, the top 1 security venue.

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.

Honors & Awards

Contest Awards

2017	Rank 1st in XMCTF.	*Xiamen, China*
2017	First Prize of National Information Security Contest.	*Shanghai, China*
2015	Rank 6th in 0CTF.	*Shanghai, China*
2014	Rank 2nd in BCTF.	*Beijing, China*

Honors

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

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

- Proposed Lynx, a Node.js vulnerability finding tool that can automatically find bugs and construct exploits.
- Discovered 15 previously unknown Node.js vulnerabilities.

Unexpected Data Dependency Creation and Chaining: A New Attack to SDN. *S&P'20*

Feng Xiao, Jinquan Zhang, Jianwei Huang, Guofei Gu, Dinghao Wu, Peng Liu

- Proposed SVHunter, an automatic vulnerability detection tool for SDN controller.
- Discovered 18 previously unknown SDN vulnerabilities.

PatternListener: Cracking Android Pattern Lock Using Acoustic Signals. *CCS'18*

Man Zhou, Qian Wang, Jingxiao Yang, Qi Li, **Feng Xiao**, Zhibo Wang, Xiaofeng Chen.

- Discovered a new side-channel which is able to leak user inputs on Android platform.

Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller. *DEFCON'18*

Feng Xiao, Jianwei Huang, Peng Liu.

- Discovered a previously unknown OpenFlow protocol design insecurity.

Enabling Secure Location Authentication in Drone (poster). *MobiCom'17*

Feng Xiao, Man Zhou, Youcheng Liye, Jingxiao Yang, Qian Wang.

- Proposed WiDrone, a multi-channel location cross-check system to mitigate GPS spoofing attacks targeted at CPS.

Education

Georgia Institute of Technology *Atlanta, USA*

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

- Working on system security with Prof. Wenke Lee.
- GPA: 4/4

Wuhan University *Wuhan, China*

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

- GPA: 3.87/4

Programming languages

Natively fluent: C, Python, Java, PHP

Conversationally fluent: JavaScript, Matlab