Feng **Xiao**

PhD. Student In Computer Science

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

Summary

First-year PhD. student at Georgia Tech. 6+ years experience specializing in the security tool development and OS hacking. Obtainted 14 CVEs from widely used software. Interested in developing proactive and adversarial approaches to protect computer systems.

Project Experience

Nodejs Program Analysis and Automatic Bug Finding — *Atlanta, USA*

Georgia Tech — *Oct. 2019 - Now*

- Discovered Hidden Parameter Attack, a new type of attack in Nodejs ecosystem.
- Built HiPar, an automatic Nodejs bug finding framework by combining dynamic data flow tracking (Jalangi) and static syntax analysis (esprima).
- Identified 5 previously unknown vulnerabilities from widely used nodejs modules (e.g., MongoDB, class-validator) and tested 60 of the most popular frameworks against them. We found that 39 of these frameworks suffers from at least one discovered vulnerability.

Test-driven Protocol Feature Identification and Debloating — *Atlanta, USA*

Georgia Tech — *Jul. 2019 - Now*

- Proposed an new method to identify and remove unwanted program logics from deployed protocol implementations.
- Built Deproto, a fully automatic protocol debloating framework combining dynamic tracing (Intel Pin) and static control flow analysis.
- Evaluated Deproto on several protocol implementations. The results indicated that Deproto is able to succuessfuly remove features from complex protocols such as OpenSSL (588+ KloC).

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

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. Co., Ltd. — *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% students nationwide)	*Wuhan, China*
2015	Yuanyi Scholarship.	*Wuhan, China*

Publication

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, a fully 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.

Wuhan University

Wuhan, China

B.S. in Computer Science

Sept. 2014 - Jun. 2018

- GPA: 3.87/4

Programming languages

Natively fluent: Python, C, Java, PHP

Conversationally fluent: JavaScript, C++, Matlab