Feng Xiao

School	Georgia Tech	**Phone**	814-7777019
Github	`https://github.com/xiaofen9` (173 stars)	**Email**	f3ixiao@gmail.com

Bio

My research interests are in **software and system security**. In particular, I am very interested in taking a proactive and adversarial approach to protect computer systems. I am also interested in the theoretical problems arising out of developing such approaches.

Education

2019-Now Ph.D. in Computer Science - Georgia Tech

2014-2018 Bachelor in Computer Science - Wuhan University

Publications

S&P'20 Unexpected Data Dependency Creation and Chaining: A New Attack to SDN.
Feng Xiao, Jinquan Zhang, Jianwei Huang, Guofei Gu, Dinghao Wu, Peng Liu.
Accepted to appear

CCS'18 PatternListener: Cracking Android Pattern Lock Using Acoustic Signals.
Man Zhou,Qian Wang,Jingxiao Yang,Qi Li, **Feng Xiao**, Zhibo Wang, Xiaofeng Chen.
Accepted

DEFCON 26 Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller.
Feng Xiao, Jianwei Huang, Peng Liu.
Accepted Video

MobiCom'17 Enabling Secure Location Authentication in Drone. (poster)
Feng Xiao, Man Zhou, Youcheng Liye, Jingxiao Yang, Qian Wang.
Accepted

SCN CHAOS: An SDN-Based Moving Target Defense System.
Yuan Shi, Huanguo Zhang, Juan Wang, **Feng Xiao**, Jianwei Huang, Daochen Zha.
Accepted

Project Experiences

- **SDN Custom Attack**

  Description: Proposed the first SDN attack that can remotely compromise SDN software stack to simultaneously cause multiple kinds of attack effects in SDN controllers.
  (Finished in Oct 2018)

  Outputs: (1) Discover 19 related 0days from 5 most popular SDN controllers, and constructs 23 exploit chains that can bring serious attack effects
  (2) Designed a backward taint analysis and logic reasoning framework to automatic detect such vulnerabolities (3,100+ LoC).
  (3) This work was accepted by the top industrial conference **DEFCON 26** as an official talk.

  Reference: DEFCON Talk Attack Video Demo

- **Windows Kernel Rootkit**

  Description: Designed a driverless method that bypasses Windows Kernel Protection (i.e., PG, DSE) on ALL Windows platform (Till April 2018).
  (Finished in April 2018)
  Outputs: Developed a comprehensive Windows all platform Rootkit (40,000+ LoC) with DNS C&C tunnel, keylogger, etc.
  Reference: No public disclosure due to ethic concerns.

- **Android App Cryptography Insecurities**

  Description: 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.
  (Finished in August 2016)
  Outputs: (1) Develop a dynamic hook framework StupidHam to semi-automatically verified such risks. to bring serious attack effects
  (2) The most serious vulnerability, found from Chinese largest food delivery company Eleme, was honored as the most valuable vulnerability by Wooyun, the biggest bug hunting community.
  Reference: Bug Disclosure on Wooyun App Injection Framework

Honors & Awards

Oct 2018 ACM CCS Student Travel Grant Award.

Nov 2017 First Prize of XMCTF (Rank 1st domestically).

Oct 2017 LeiJun Scholarship (Top 1 out of 310).

Dec 2016 **National Scholarship** (The highest student honor in China, awarded to top 0.2% students nationwide).

Aug 2016 First Prize of National Undergraduate Information Security Contest.

Oct 2015 Yuanyi Scholarship (Top 1 out of 310).

Apr 2015 Third Prize of 0CTF (Rank 6th internationally).

Dec 2014 First Prize of BCTF (Rank 2nd domestically).

Work Experiences

Aug 2017 - Sep 2017 Security Platform Department, Tencent
Internship
Security Engineer

- I proposed a new XSS mitigation method leveraging the feature of Content Security Policy, and the method is gradually deploying in all servers of Tencent.
- I captured and mitigate one 0day attack (CVE 2017-9805) towards our companies' servers, and I found 8 high risk vulnerabilities from the products of Tencent.

Vulnerability I discovered

CVE-2018-1132 Opendaylight's SDNInterfaceapp SQL injection.
CVE-2018-15595 Opendaylight's TSDR Denial of Service.
CVE-2018-1999020 ONOS Controller Directory Traversal.
CVE-2018-1000614 ONOS Controller Notification XXE.
CVE-2018-1000615 ONOS Controller OVSDB Remote Denial of Service.
CVE-2018-1000616 ONOS Controller XMLCONFIGPARSER XXE.
CVE-2018-1000617 Atlassian Floodlight Controller Remote Denial of Service.
CVE-2018-1000163 Atlassian Floodlight Controller Web Console Cross-Site Scripting.