Xiaochen Zou / 邹笑尘

Last updated: January, 2022
Email: xzou017@ucr.edu
Website: etenal.me
Github: github.com/plummm

Computer Science and Engineering
University of California, Riverside
Advised by Prof. Zhiyun Qian

RESEARCH INTEREST

My current research focus **Linux kernel fuzzing and vulnerability exploit**. I'm curious about bug hunting technique and vulnerability mitigation strategy, and based on such knowledge, building a more robust operating system and making contribution to the community. **Program analysis** is another field I've been working on, a security tool I built upon symbolic execution and static taint analysis, that detects the security impacts of kernel bugs, received multiple credit from different Linux kernel communities.

My future research will sit on the same direction, but also introducing the help of **Machine Learning**. I believe Machine Learning can perfectly assist human expert in solving security issues associated with decision making(fuzzing seeds mutation), intrusion detection(firewall rules), and so many.

EDUCATION

2021 – present **Ph.D. in Cyber Security**
University of California, Riverside, USA
PI: Zhiyun Qian

2019 – 2021 **M.S in Computer Science**
University of California, Riverside, USA
GPA : 3.51/4

2015 – 2019 **Bachelor in Computer Science**
University of Electronic Science and Technology of China, PRC
GPA : 3.22/4

SKILLS

Programming C/C++/GO/Python

Security Reverse Engineering/Kernel Exploit
Program Analysis/Kernel Fuzzing

Others Windows/Linux Kernel

PUBLICATIONS

PAPERS

2022

[C4] **SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel**
Xiaochen Zou, Guoren Li, Weiteng Chen, Hang Zhang, Zhiyun Qian
USENIX Security 2022 (To appear)
• PDF https://www.usenix.org/system/files/sec22summer_zou.pdf

2021

[C3] **Eluding ML-based Adblockers With Actionable Adversarial Examples**
Shitong Zhu, Zhongjie Wang, Xun Chen, Shasha Li, Keyu Man, Umar Iqbal, Zhiyun Qian, Kevin S. Chan, Srikanth V. Krishnamurthy, Zubair Shafiq, Yu Hao, Guoren Li, Zheng Zhang, **Xiaochen Zou**
Annual Computer Security Applications Conference (ACSAC 21)
• PDF https://www.shitong.me/pdfs/acsac21_a4.pdf

[C2] **Statically Discovering High-Order Taint Style Vulnerabilities in OS Kernels**
Hang Zhang, Weiteng Chen, Yu Hao, Guoren Li, Yizhuo Zhai, **Xiaochen Zou**, Zhiyun Qian
2021 ACM SIGSAC Conference on Computer and Communications Security (CCS 21)
• PDF https://www.cs.ucr.edu/ zhiyunq/pub/ccs21_static_high_order.pdf

2020

[C1] **KOOBE: Towards Facilitating Exploit Generation of Kernel Out-Of-Bounds Write Vulnerabilities**
Weiteng Chen, **Xiaochen Zou**, Guoren Li, Zhiyun Qian
USENIX Security 2020
• PDF https://www.usenix.org/system/files/sec20-chen-weiteng.pdf

EVENTS

CONTEST

2021

[C8] **Exploited the LAN interface of the NETGEAR R6700v3 router**
Pwn2Own 2021 Austin

2018

[C7] **3th in 2018 National Cyber Security Contest of College Students of China**

[C6] **3th in 2018 Qiangwang Cyber Security Contest**

2017

[C5] **5th in 2017 DDCTF**
Nationwide Individual Capture The Flag Contest with 4000 contestants

[C4] **7th in 2017 0ctf**

[C3] **1st in 2017 Anheng national security competition in west-south district**

2016

[C2] **1st in 2016 Anheng national security competition in west-south district**

2013

[C1] **1st prize of National Olympiad in Informatics in Provinces(NOIP)**
National Olympiad in Informatics in Provinces(NOIP) 2013

INVITED TALKS

[T1] **SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs inLinux kernel**
Linux Security Summit 2021 Seattle

LEADERSHIP

2015-2016 **Cohesion Network Security Studio**
Team Leader
https://blog.cnss.io/

PROFESSIONAL EXPERIENCE

2016 **DiDi—Beijing, China**
Cyber Security Intern
Analyze malware and extract characteristics to build internal security firewall

AWARDS & HONORS

2021
- Exploiting the LAN interface of the NETGEAR R6700v3 router in Pwn2Own 2021 Austin
- LSS 2021 Travel Grant Award

2019
- Dean's Distinguished Fellowship Award

VULNERABILITIES CREDITS

2021 CVE-2021-42008 (LPE on Ubuntu)
CVE-2021-33034
CVE-2021-33033
CVE-2020-36387 (Control flow hijacking in Linux kernel)
CVE-2020-36386
CVE-2020-36385 (Control flow hijacking in Linux kernel)
CVE-2020-36387
CVE-2019-25044 (Control flow hijacking in Linux kernel)
CVE-2018-25015 (Control flow hijacking in Linux kernel)
CVE-2019-25045 (Control flow hijacking in Linux kernel)

PROJECTS

[P3] **SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel**
183 high-risk bugs identified
https://github.com/plummm/SyzScope

[P2] **Anti-Revoke Tools for Wechat, Telegram, and QQ**
375 stars up until 2022
https://github.com/plummm/AntiRecall

[P1] **Cryptocurrency Converter**
73 stars up until 2022
https://github.com/plummm/alfred3-workflow-CurrencyX

SUB-REVIEW

USENIX Security	’22 Fall, ’21 Winter
IEEE S&P	’21 Fall
NDSS	’21 Fall, ’20 Fall