

# Xiaochen Zou (Shee-ow Chen Zoh) / 邹笑尘

---

Last updated: December, 2023

Email: [etenal@etenal.me](mailto:etenal@etenal.me)

Website: [etenal.me](http://etenal.me)

Github: [github.com/plummm](https://github.com/plummm)

Twitter: [@etenal7](https://twitter.com/etenal7)

Linkedin: [xiaochen-zou](https://www.linkedin.com/in/xiaochen-zou)

Computer Science and Engineering

University of California, Riverside

Advised by Prof. Zhiyun Qian

## EDUCATION

2019 – present **Ph.D. in Cyber Security (anticipate graduating by Spring 2025)**

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/Bash/Assembly code

Security Reverse Engineering (IDA, GDB, x64dbg, Windbg) /Kernel Exploit (Linux)

Program Analysis (LLVM, angr) /Fuzzing (syzkaller, AFL)

Others Windows/Linux/Git/Docker

## PROFESSIONAL EXPERIENCE




2019 - Present **University of California, Riverside – Riverside, USA**


Security Research Assistant

My current research focus is on Linux kernel fuzzing and vulnerability exploit. I have developed multiple security tools based on program analysis techniques like **symbolic execution** and **static taint analysis**, the tools reveal the security impacts of Linux kernel vulnerabilities for both upstream and downstream systems. By utilizing my knowledge of Linux kernel, I have a track record of successfully developing multiple Linux kernel exploits in the past, leading to local privilege escalation on the latest Ubuntu kernel.

- 2022 Jun-Sep **Samsung Research America – Mountain View, USA**  
Security Research Intern  
Utilize my professional experience in Windows security engineering to craft PoCs for testing internal security tools and Samsung Knox driver, which **prevents potential unsafe behavior** on the company's devices and **protects the company's intellectual knowledge from unsafe leaking**. At the same time, I also led a separate research on Windows LOLBin discovery and managed to find one new LOLBin attack surface in Windows office software.
- 2017 Jun-Sep **DiDi – Beijing, China**  
Cyber Security Intern  
**Reverse engineer** prevalent malware and ransomware, extracting their network traffic characteristics. Building an internal database to help the firewall detect and block suspicious network traffic in the company network.

## PROJECTS

- [P4] **SyzBridge: Bridging the Gap in Exploitability Assessment of Linux Kernel Bugs in the Linux Ecosystem**  
*Python, C, Golang, Bash Script*  
[\[CVE-2022-27666\]](#) [\[CVE-2021-42008\]](#)  
SyzBridge provides the possibility of bringing Linux upstream kernel bug PoCs to the downstream kernels. It is a fully automatic system that adapts upstream PoCs by tuning race condition, removing unnecessary setup, and loading missing kernel modules. SyzBridge can easily integrate with existing bug assessment tools like SyzScope. The integrated pipe managed to discover 50+ highly exploitable bugs on downstream kernels (e.g., Ubuntu, Debian, Fedora, and Suse).
  - Code:  [plummm/SyzBridge](#)
- [P3] **SyzScope: Revealing High-Risk Security Impacts of Fuzzer-Exposed Bugs in Linux kernel**  
*Python, C, Golang, Bash Script*  
[\[CVE-2021-33034\]](#) [\[CVE-2021-33033\]](#) [\[CVE-2020-36387\]](#) [\[CVE-2020-36386\]](#) [\[CVE-2020-36385\]](#)  
[\[CVE-2020-36387\]](#) [\[CVE-2020-36387\]](#) [\[CVE-2019-25044\]](#) [\[CVE-2018-25015\]](#) [\[CVE-2019-25045\]](#)  
SyzScope is a system that can automatically uncover high-risk impacts of a given Linux kernel bug with only low-risk impacts. It utilizes static taint analysis, symbolic execution, and fuzzing techniques to reveal the potential high-risk bugs among seemingly low-risk bugs from syzbot. The results revealed 183 previous unknown high-risk bugs.
  - Code:  [plummm/SyzScope](#)
- [P2] **Anti-Revoke Tools for Wechat, Telegram, and QQ**  
*C#, C*  
A tool that can prevent deleting messages in several messenger apps like WeChat, Telegram and QQ. 525 stars up until 2023
  - Code:  [plummm/AntiRecall](#)

- [P1] **Cryptocurrency Converter**  
*Python*  
78 stars up until 2022
- Code:  [plummm/alfred3-workflow-CurrencyX](https://github.com/plummm/alfred3-workflow-CurrencyX)




## PUBLICATIONS

### PAPERS


2024

- [C8] **SyzBridge: Bridging the Gap in Exploitability Assessment of Linux Kernel Bugs in the Linux Ecosystem**  
Xiaochen Zou, Yu Hao, Zheng Zhang, Juefei Pu, Weiteng Chen, Zhiyun Qian  
*The Network and Distributed System Security Symposium (NDSS) 2024 (To be appeared)*
- PDF  <https://etenal.me/download/SyzBridge.pdf>
  - Code:  [seclab-ucr/SyzBridge](https://github.com/seclab-ucr/SyzBridge)
- [C7] **K-LEAK: Towards Automating the Generation of Multi-Step Infoleak Exploit against Linux Kernel**  
Zhengchuan Liang, Xiaochen Zou, Chengyu Song, Zhiyun Qian  
*The Network and Distributed System Security Symposium (NDSS) 2024 (To be appeared)*
- [C6] **SyzGen++: Dependency Inference for Augmenting Kernel Driver Fuzzing**  
Weiteng Chen, Yu Hao, Zheng Zhang, Xiaochen Zou, Dhilung Kirat, Shachee Mishra, Douglas Schales, Jiyong Jang, Zhiyun Qian  
*IEEE Security and Privacy (Oakland) 2024 (To be appeared)*

2023

- [C5] **SyzDescribe: Principled, Automated, Static Generation of Syscall Descriptions for Kernel Drivers**  
Yu Hao, Guoren Li, Xiaochen Zou, Weiteng Chen, Shitong Zhu, Zhiyun Qian, and Ardalán Amiri Sani  
*IEEE Security and Privacy (Oakland) 2023*
- PDF  [https://www.cs.ucr.edu/~zhiyunq/pub/oakland23\\_syzdescribe.pdf](https://www.cs.ucr.edu/~zhiyunq/pub/oakland23_syzdescribe.pdf)
  - Talk  [Linux Security Summit 2023] [Qualcomm Security Summit 2023]
  - Code:  [seclab-ucr/SyzDescribe](https://github.com/seclab-ucr/SyzDescribe)

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  
**Google Research Scholar Program Reward \$1,337**  
*USENIX Security 2022*
- PDF  [https://www.usenix.org/system/files/sec22summer\\_zou.pdf](https://www.usenix.org/system/files/sec22summer_zou.pdf)
  - Talk  [Linux Security Summit 2021]
  - Code:  [plummm/SyzScope](https://github.com/plummm/SyzScope)

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](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](https://www.cs.ucr.edu/~zhiyunq/pub/ccs21_static_high_order.pdf)  
 • Code:  [seclab-ucr/SUTURE](https://github.com/seclab-ucr/SUTURE)

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>  
 • Talk  [Linux Security Summit 2021]  
 • Code:  [seclab-ucr/KOOBE](https://github.com/seclab-ucr/KOOBE)

## INVITED TALKS

- [T1] **Scrutinizing bugs found by syzbot**  
 Linux Security Summit 2021 Seattle  
[\[Article\]](#) [\[Video\]](#) [\[Slides\]](#)

## AWARDS & HONORS & CTF

- |      |   |
|------|---|
| 2023 | <ul style="list-style-type: none"> <li>• Google Research Scholar Program Reward</li> <li>• Dissertation Year Program (DYP) Fellowship</li> </ul>                                |
| 2021 | <ul style="list-style-type: none"> <li>• Exploiting the LAN interface of the NETGEAR R6700v3 router in Pwn2Own 2021 Austin</li> <li>• LSS 2021 Travel Grant Award</li> </ul>    |
| 2019 | <ul style="list-style-type: none"> <li>• Dean's Distinguished Fellowship Award</li> </ul>   |
| 2018 | <ul style="list-style-type: none"> <li>• 3th in 2018 National Cyber Security Contest for College Students of China</li> </ul>   |
| 2017 | <ul style="list-style-type: none"> <li>• 5th in DDCTF among 4000 contestants</li> <li>• 7th in 2017 Octf</li> <li>• 1st in 2017 Anheng national security competition</li> </ul> |
| 2016 | <ul style="list-style-type: none"> <li>• 1st in 2016 Anheng national security competition</li> </ul>  |
| 2013 | <ul style="list-style-type: none"> <li>• 1st in National Olympiad in Informatics in Provinces(NOIP)</li> </ul>  |

## VULNERABILITIES CREDITS

- 2022 [CVE-2022-27666](#) Local privilege escalation on Ubuntu kernel 21.04  
[CVE-2022-27645](#) Bypass authentication on NETGEAR R6700v3 routers.
- 2021 [CVE-2021-42008](#)  
CVE-2021-33034  
CVE-2021-33033  
CVE-2020-36387  
CVE-2020-36386  
CVE-2020-36385  
CVE-2020-36387  
CVE-2019-25044  
CVE-2018-25015  
CVE-2019-25045

## LEADERSHIP

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

## REVIEW

- SecureComm 2023
- USENIX '22 Fall, '21 Winter  
Security
- IEEE S&P '21 Fall
- NDSS '21 Fall, '20 Fall