

Bonan Ruan

Ph.D. Candidate

School of Computing
National University of Singapore (NUS)
COM3-02-18, Singapore 119391
☎ +65 8790 6443
✉ bonan.ruan@u.nus.edu
🌐 profile.wohin.me
🔗 brant-ruan
🆔 0009-0004-5500-6060

Research Interests

My research interests mainly lie in the interactions of system security, program analysis, and AI, with a focus on developing practical and effective solutions to improve the security of various real-world **systems**. Specifically, my work centers around **vulnerabilities**, including their discovery, analysis, assessment, and defense, by leveraging and advancing various techniques, including program analysis, fuzzing, and AI.

In addition, I also have a strong interest in interdisciplinary research that bridges technical and societal perspectives, such as AI governance and the social implications of cybersecurity risks and incidents.

Education

- Jan 2024 – **Ph.D. Candidate**, *National University of Singapore (NUS)*, Singapore
Present Major: Computer Science, School of Computing
Advisor: Dr. Zhenkai Liang
GPA: 4.96/5.0
- Aug 2022 – **M.Comp.**, *National University of Singapore (NUS)*, Singapore
Dec 2023 Major: Computer Science, School of Computing
Advisor: Dr. Zhenkai Liang
GPA: 4.41/5.0
- Sep 2014 – **B.Eng.**, *Tongji University*, Shanghai, China
Jun 2019 Major: Information Security, School of Electronic and Information Engineering
Advisor: Dr. Zhijun Ding
GPA: 85.12/100

Experience

- Sep 2022 – **Research Assistant Intern**, *National Cybersecurity R&D Lab (NCL)*, Singapore
Apr 2023 Worked on educational cyber range development.
- Jul 2019 – **Security Researcher**, *NSFOCUS, Inc.*, Beijing, China
Jul 2022 Worked on cloud computing security research & product development.
- Jul 2017 – **Software Engineer Intern**, *Huawei, Ltd.*, Shanghai, China
Aug 2017 Worked on Network Function Virtualization (NFV) project development.

Publications

Book Chapters:

- **Cloud Native Security: Practice and Architecture**
Wenmao Liu, Guolong Jiang, Ming Pu, **Bonan Ruan**, Xiaohu Ye
Beijing: China Machine Press. ISBN: 9787111691839. 2021.
Contributed Chapters: 3, 4, 14, and 16.

Conferences and Workshops:

- **Fuzzing the PHP Interpreter via Dataflow Fusion**
Yuancheng Jiang, Chuqi Zhang, **Bonan Ruan**, Jiahao Liu, Manuel Rigger, Roland Yap, Zhenkai Liang
USENIX Security Symposium, 2025.

- **KernJC: Automated Vulnerable Environment Generation for Linux Kernel Vulnerabilities**
Bonan Ruan, Jiahao Liu, Chuqi Zhang, Zhenkai Liang
International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2024.
Best Practical Paper Award
- **VulZoo: A Comprehensive Vulnerability Intelligence Dataset**
Bonan Ruan, Jiahao Liu, Weibo Zhao, Zhenkai Liang
IEEE/ACM International Conference on Automated Software Engineering Tool (ASE), 2024.
- **Security Challenges in the Container Cloud**
Yutian Yang, Wenbo Shen, **Bonan Ruan**, Wenmao Liu, Kui Ren
IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2021.

Patents

- CN111835768 A Method, Apparatus, Medium, and Device for Handling Security Incidents
- CN112035839 A Method and Apparatus for Detecting Race Condition Vulnerability Exploitation
- CN111831275 A Method, Server, Medium, and Device for Orchestrating Micro-Scenario Scripts
- CN112153049 An Intrusion Detection Method, Apparatus, Device, and Computer-Readable Medium
- CN115103362 A Method, Apparatus, and Device for Restoring 5G Network Element Call Sequences

Open-Source Softwares

- KernJC An automated vulnerable environment generation tool for Linux kernel vulnerabilities, which is capable of constructing reproducible, vulnerable environments, where the real vulnerable kernel version is compiled with the correct kernel configs to make the vulnerability available and triggerable. Repo: <https://github.com/NUS-Curiosity/KernJC>.
- VulZoo A large-scale vulnerability intelligence dataset that integrates various sources of structural and non-structural data, aiming to interconnect individual intelligence and provide the most comprehensive profiling of vulnerabilities for downstream tasks, e.g., vulnerability detection, assessment, and prioritization. Repo: <https://github.com/NUS-Curiosity/VulZoo>.
- Metarget A framework providing automatic multi-level vulnerable cloud native environments. Metarget has received over 1.2k GitHub stars and is listed in the CNCF Landscape. Repo: <https://github.com/Metarget/metarget>.

Talks and Speeches

- **KernJC: Automated Vulnerable Environment Generation for Linux Kernel Vulnerabilities**
(Industry) BlackHat Asia 2025, Singapore
- **VulZoo: A Comprehensive Vulnerability Intelligence Dataset**
ASE 2024, Sacramento, USA
- **KernJC: Automated Vulnerable Environment Generation for Linux Kernel Vulnerabilities**
RAID 2024, Padua, Italy
- **Dilemma: runC's Achilles' Heel**
(Industry) KCon 2022, Beijing, China
- **Metarget: Auto-Construction of Vulnerable Cloud Native Infrastructure**
(Industry) OpenInfraDays Asia 2021, Online
- **k0otkit: A Universal Manipulation Technique in Post-Penetration against Kubernetes**
(Industry) CIS 2020, Shanghai, China

Teaching and Mentoring

- 2025 Fall Teaching Assistant for CS5231 System Security, NUS

2025 Spring Teaching Assistant for CS5321 Network Security, NUS
2024 Fall Teaching Assistant for CS5231 System Security, NUS

Selected Awards

2024 Best Practical Paper Award, RAID 2024
2024 NUS Research Scholarship
2023 Student Scholarship, BlackHat Asia 2023
2017 Cybersecurity Scholarship, China Internet Development Foundation
2017 Tongji Scholarship of Excellence (2nd prize)

Academic Services

2025 External reviewer for CCS 2025