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

Bonan Ruan

Ph.D. Candidate

Research Interests

My research interests mainly lie in the interactions of system security, program analysis, and Large Language Models (LLMs), with a focus on developing practical and effective solutions to improve the security of various real-world ***systems*** and ***software supply chains***. Currently, I am investigating the security of LLM-based agentic systems, focusing on uncovering, detecting, and mitigating emerging threats from the perspectives of both vulnerabilities and anomalies.

Education

Jan 2024 – Present **Ph.D. Candidate**, *National University of Singapore (NUS)*, Singapore
Major: Computer Science, School of Computing
Advisor: Prof. Zhenkai Liang (homepage)
GPA: 4.94/5.0

Aug 2022 – Dec 2023 **M.Comp.**, *National University of Singapore (NUS)*, Singapore
Major: Computer Science, School of Computing
Advisor: Prof. Zhenkai Liang
GPA: 4.41/5.0

Sep 2014 – Jun 2019 **B.Eng.**, *Tongji University*, Shanghai, China
Major: Information Security, School of Electronic and Information Engineering
Advisor: Prof. Zhijun Ding (homepage)
GPA: 85.12/100

Experience

Sep 2022 – Apr 2023 **Research Intern**, *National Cybersecurity R&D Lab (NCL)*, Singapore
Worked on educational cyber range development.

Jul 2019 – Jun 2022 **Security Researcher**, *NSFOCUS, Inc.*, Beijing, China
Worked on cloud computing security research & product development.

Jul 2017 – Aug 2017 **Software Engineer Intern**, *Huawei, Ltd.*, Shanghai, China
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.

Preprints:

- **Heimdallr: Characterizing and Detecting LLM-Induced Security Risks in GitHub CI Workflows**
  Bonan Ruan, Yeqi Fu, Chuqi Zhang, Jiahao Liu, Jun Zeng, Zhenkai Liang
  arXiv. May 2026.

- **TraceAegis: Securing LLM-Based Agents via Hierarchical and Behavioral Anomaly Detection**

Jiahao Liu, **Bonan Ruan**, Xianglin Yang, Zhiwei Lin, Yan Liu, Yang Wang, Tao Wei, Zhenkai Liang
arXiv. October 2025.

- **When MCP Servers Attack: Taxonomy, Feasibility, and Mitigation**
  Weibo Zhao, Jiahao Liu, **Bonan Ruan**, Shaofei Li, Zhenkai Liang
  arXiv. September 2025.

Conferences:

- **DevOpsGym: Benchmarking AI Agents in Software DevOps Cycle**
  Yuheng Tang*, Kaijie Zhu*, **Bonan Ruan**, Chuqi Zhang, Michael Yang, Hongwei Li, Suyue Guo, Tianneng Shi, Zekun Li, Christopher Kruegel, Giovanni Vigna, Dawn Song, William Yang Wang, Lun Wang, Yangruibo Ding, Zhenkai Liang, Wenbo Guo
  *International Conference on Learning Representations (**ICLR**) 2026.*

- **Propagation-Based Vulnerability Impact Assessment for Software Supply Chains**
  Bonan Ruan, Zhiwei Lin, Jiahao Liu, Chuqi Zhang, Kaihang Ji, Zhenkai Liang
  *IEEE/ACM International Conference on Automated Software Engineering (**IEEE/ACM ASE**) 2025.*

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

- **A Large-Scale Evolvable Dataset for Model Context Protocol Ecosystem and Security Analysis**
  Zhiwei Lin, **Bonan Ruan**, Jiahao Liu, Weibo Zhao
  *IEEE/ACM International Conference on Automated Software Engineering Tool (**IEEE/ACM ASE**) 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 (**IEEE/ACM 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 (**IEEE TPS**) 2021.*

Workshops:

- **Towards Trusted Extensible Device Measurement and Management via Intra-Firmware Privilege Isolation**
  Chuqi Zhang, **Bonan Ruan**, Vikram Ramaswamy, Zhenkai Liang, Adil Ahmad
  Workshop on Operating System Research for Connected Intelligence (WoSCI, co-located with ASPLOS/EuroSys), 2025.

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 Software

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 automatical constructions multi-level vulnerable cloud native environments. Metarget has received over 1.3k GitHub stars and is listed in the CNCF Landscape. Repo: `https://github.com/Metarget/metarget`.

Talks and Speeches

- **Propagation-Based Vulnerability Impact Assessment for Software Supply Chains**
  ASE 2025, Seoul, South Korea
- **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, 2026 Teaching Assistant for CS5321 Network Security, NUS

2024, 2025 Teaching Assistant for CS5231 System Security, NUS

Selected Awards

2025 Research Achievement Award, School of Computing, NUS

2025 Distinguished Paper Award, USENIX Security 2025

2024 Best Practical Paper Award, RAID 2024

2024 NUS Research Scholarship

2023 Student Scholarship, BlackHat Asia 2023

2017 Cybersecurity Scholarship, China Internet Development Foundation (Link)

2017 Tongji Scholarship of Excellence (2nd Prize)

2016 2nd Prize in Tongji Information Security Competition

Academic Services

2026 Artifact Evaluation reviewer for USENIX Security

2026 External reviewer for ACM ASIACCS

2025 External reviewer for ACM CCS