

# 王子成

✉ wzc@smail.nju.edu.cn      🌐 <https://www.zi-c.wang/>

✉ TEL/WeChat:15754311250      ✉ +17202182926

## 研究

操作系统内核安全是我主要的研究方向，包括内核漏洞响应和内核安全敏感对象隔离。

目前研究重点聚焦于 **eBPF** 内核内虚拟机，探索如何利用其沙箱、内核旁路等特性，提升内核的安全和性能表现。

## 经历

- 2018 – 2024      📌 博士, 南京大学 软件新技术国家重点实验室.  
研究方向: 操作系统安全, 内核漏洞  
导师: 曾庆凯教授
- 2023 – 2024      📌 学术交流, **University of Colorado Boulder** Computer Science Department.  
研究方向: *eBPF* 赋能内核安全研究  
导师: Prof. Yueqi Chen
- 2014 – 2018      📌 本科, 吉林大学 软件学院.  
研究方向: 软件加壳

## 发表

### 会议

- 1      **Zicheng Wang**, Y. C., & Zeng, Q. (n.d.). Practical eBPF Reference Monitor(8 月投稿). In *ASPLOS (CCF-A)*.
- 2      Chen, Y., Lin, M., Lin, C., Wang, J., **Zicheng Wang**, & Shen, M. (2023). Kill Latest MPU-based Protections in Just One Shot: Targeting All Commodity RTOSes. In *Black hat USA*.
- 3      Chen, Y., **Zicheng Wang**, Lin, Z., Le, M., Le, D., Jiang, Y., ... Jamjoom, H. (2023). HotBPF: Nip Kernel Heap-based Exploitation in the Bud (审稿中). In *CCS (CCF-A)*.
- 4      **Zicheng Wang**, & Chen, Y. (2023). HotBPF++: A More Powerful Memory Protection for the Linux Kernel. In *Linux Security Summit North America*. \*\$1600 旅行基金奖励.
- 5      **Zicheng Wang**, Y. C., & Zeng, Q. (2023). PET: Prevent Discovered Errors from Being Triggered in the Linux Kernel. In *Usenix Security (CCF-A)*.
- 6      Bingnan, Z., **Zicheng Wang**, Guo, Y., & Qingkai, Z. (2022). CryptKSP: A Kernel Stack Protection Model Based on AES-NI Hardware Feature. In *IFIP SEC (CCF-C)*.
- 7      Yinggang, G., **Zicheng Wang**, Bingnan, Z., & Qingkai, Z. (2022). Formal Modeling and Security Analysis for Intra-level Privilege Separation. In *ACSAC (CCF-B)*.



### 期刊

- 1 **Zicheng Wang**, Yinggang, G., Bingnan, Z., Yueqi, C., & Qingkai, Z. (2023). 基于 eBPF 的内核堆漏洞动态缓解研究. *JOS: 软件学报 (中文 CCF-A)*.





## 专利

- 1 Yueqi Chen and **Zicheng Wang**. (2023). An Infrastructure For Preventing Compromise of Operating System Kernels Due to Discovered Errors. **US Patent 63/464,887** 美国专利.

## 技能

- 学术研究     理解并提取研究问题背后的原理，发现并提出新的见解，善于合作沟通。
- 操作系统安全     掌握服务器 Linux、嵌入式 FreeRTOS 等操作系统的结构以及各个子系统的功能和实现。熟悉有关 intel CPU 硬件机制和虚拟化技术的细节。结合静态程序分析和动态调试，理解并复现公开内核漏洞。

## 开源

- ERA     An eBPF-assisted Randomization Allocator to prevent kernel heap vulnerabilities.
- PET     An eBPF framework to prevent discovered errors from being triggered.
- TA-BattleEinsteinChess     A robust EinsteinChess battle server, support more than 200 connections on a desktop.
- CCFrank4dblp     Displays the China Computer Federation (CCF) recommended rank of conferences and journals in the dblp, Google Scholar, Connected Papers and Web of Science search results.

王子成  
最后更新: 2023-07-04