

# Zicheng Wang

✉ wzc@smail.nju.edu.cn

🌐 <https://www.zi-c.wang/>

📞 +1 7202182926

☎ 15754311250

## Research Interest

My research focuses on **Operating System Kernel Security**, specifically in the areas of kernel vulnerabilities prevention and isolation/compartimentalization techniques.

Recently I am researching on **eBPF**, an innovative in-kernel virtual machine, to enhance both the security and performance aspects of the kernel.

## Education

- 2018 – 2024    📖 **Ph.D. Candidate, Nanjing University** Computer Science.  
Research Interest: *Operating System Bugs, Kernel Isolation*
- 2023 – 2024    📖 **Research Assistant, University of Colorado Boulder** Computer Science Dept.  
Research Interest: *eBPF framework*
- 2014 – 2018    📖 **B.Eng. Jilin University** College of Software.  
Research Interest: *Software Packer*

## Publications

### Conference

- 1    **Zicheng Wang**, Chen, Y., & Zeng, Q. (2023). PET: Prevent Discovered Errors from Being Triggered in the Linux Kernel. In *Usenix Security*.
- 2    **Zicheng Wang**, & Chen, Y. (2023). HotBPF++: A More Powerful Memory Protection for the Linux Kernel. In *Linux Security Summit North America*. \*\$1600Linux Foundation funding.
- 3    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*.
- 4    Yinggang, G., **Zicheng Wang**, Bingnan, Z., & Qingkai, Z. (2022). Formal Modeling and Security Analysis for Intra-level Privilege Separation. In *ACSAC*.
- 5    Zhong, B., **Zicheng Wang**, Guo, Y., & Zeng, Q. (2022). CryptKSP: A Kernel Stack Protection Model Based on AES-NI Hardware Feature. In *IFIP SEC*.
- 6    Sun, R., Guo, Y., **Zicheng Wang**, & Zeng, Q. (2023). AttnCall: Refining Indirect Call Targets in Binaries with Attention. In *ESORICS*.
- 7    Chen, Y., **Zicheng Wang**, Lin, Z., Le, M., Le, D., Jiang, Y., ... Jamjoom, H. (n.d.). HotBPF: Nip Kernel Heap-based Exploitation in the Bud (To be submitted).



### Journal

- 1 **Zicheng Wang**, Yinggang, G., Bingnan, Z., Yueqi, C., & Qingkai, Z. (2023). A Research on eBPF Based Dynamic Mitigation for Kernel Heap Vulnerabilities. *JOS: Journal of Software*.



## Patent

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





## Skills

- Academic Research     Understand and extract the rationale behind research questions, discover and present new insights...
- Operation System     Master the architecture of the server/IOT operating systems and the functions and implementation of subsystems. Familiar with details about intel CPU and virtualization technology. Understand the static and dynamic program analysis and replay publicly reported kernel bugs.

## Teaching Experience

- 2018 Autumn     **Advanced Object Oriented Programming** as TA for undergraduates.
- 2019 Summer     **Assembly Programming** as TA for undergraduates.

## Open Source

- 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.

Zicheng Wang  
update: 2023-08-17