



Yinggang Guo



✉ gyg@smail.nju.edu.cn

Education




- 2019 – present  **Ph.D. student, Nanjing University**, Dept. of Computer Science and Technology.
Research Interests: *OS Kernel Security, Privilege Separation, Formal Modeling.*
- 2015 – 2019  **B.Eng., Nankai University**, College of Software.
Research Interests: *Control-Flow Integrity.*

Publications

Conference Proceedings

- 1 **Y. Guo**, Z. Wang, B. Zhong, and Q. Zeng, “Formal modeling and security analysis for intra-level privilege separation,” in *Proceedings of the 38th Annual Computer Security Applications Conference*, ser. ACSAC ’22, Austin, TX, USA, 2022, pp. 88–101.  DOI: 10.1145/3564625.3567984.
- 2 B. Zhong, Z. Wang, **Y. Guo**, and Q. Zeng, “Cryptksp: A kernel stack protection model based on aes-ni hardware feature,” in *ICT Systems Security and Privacy Protection: 37th IFIP TC 11 International Conference*, ser. SEC ’22, Copenhagen, Denmark, 2022, pp. 270–286.  DOI: 10.1007/978-3-031-06975-8_16.

Skills

- Operating System  Solid foundation in operating system; familiar with hardware features such as Intel PKU/PKS, WP, NXE, SMAP, and their application in system isolation.
- Formal Modeling  Good at thinking formally; familiar with model-driven security analysis; skilled in B-method, and experienced in model checking using ProB.
- Misc.  Self-motivated, strong ability to organize and analyze problems, with a keen interest in system security ...

Teaching Experience

- 2022 Spring  **Introduction to the Software Industry** as TA for undergraduates.
- 2020 Summer  **Assembly Programming** as TA for undergraduates.

Projects

- Privilege-Centric Model **A general and extensible formal framework** for intra-level privilege separation systems, consisting of a privilege-centric model (PCM) and security invariants based on privilege differences. Model checking for Nested Kernel, Hilps, SKEE, and SelMon in **ProB**. <https://github.com/gyg128/Privilege-Centric-Model>
- Kernel Compartmentalization **Hardware-assisted kernel compartmentalization** based on the principle of least privilege. On the mechanism level, I am exploring the use of **Intel PKS** and **NXE** features for secure isolation, preventing both memory corruption and control flow hijacking. On the policy level, I believe that **type-based dependence analysis** will be a promising approach.