Yinggang Guo

gyg@smail.nju.edu.cn 15122609660
https://gyg128.github.io/ gyg128_wx

Research Interests

My research focuses on **Operating System Kernel Security**, including **privilege separation** and **kernel compartmentalization**. My research goal is to enhance kernel security based on **the principle of least privilege**. I have analyzed the security effects of various privilege separation schemes through formal modeling. Recently, I am working on secure, scalable, and efficient kernel compartmentalization, combining advanced hardware features and program analysis techniques to confine the impact of vulnerabilities.

Education

2019 – 2025 **Ph.D. Student, Nanjing University**, State Key Lab for Novel Software Technology.
Research Interests: *OS Kernel Security, Formal Modeling.*
Supervisor: Prof. Qingkai Zeng

2023 – 2024 **Visiting Scholar, University of Minnesota**, Dept. of Computer Science & Engineering.
Research Interests: *Kernel Compartmentalization.*
Supervisor: Prof. Kangjie Lu

2015 – 2019 **B.Eng., Nankai University**, College of Software. *Excellent Undergraduate Student Award.*
Research Interests: *Control-Flow Integrity.*

Publications

Conference Proceedings

1. **Yinggang Guo**, Z. Wang, W. Bai, Q. Zeng, and K. Lu, "BULKHEAD: Secure, Scalable, and Efficient Kernel Compartmentalization with PKS," in *NDSS'25* ***(CCF-A)***, 2025. DOI: `10.14722/ndss.2025.23328`.
2. **Yinggang Guo**, Z. Wang, B. Zhong, and Q. Zeng, "Formal Modeling and Security Analysis for Intra-level Privilege Separation," in *ACSAC'22* ***(CCF-B)***, 2022. DOI: `10.1145/3564625.3567984`.
3. R. Sun, **Yinggang Guo**, Z. Wang, and Q. Zeng, "AttnCall: Refining Indirect Call Targets in Binaries with Attention," in *ESORICS'23* ***(CCF-B)***, 2023. DOI: `10.1007/978-3-031-51482-1_20`.
4. Z. Wang, **Yinggang Guo**, Y. Chen, and Q. Zeng, "ERA: Dynamic Mitigation Solution Based on eBPF Against Kernel Heap Vulnerabilities," in *China Linux Kernel Developer Conference CLK'23*, 2023.
5. B. Zhong, Z. Wang, **Yinggang Guo**, and Q. Zeng, "CryptKSP: A Kernel Stack Protection Model Based on AES-NI Hardware Feature," in *IFIP SEC'22* ***(CCF-C)***, 2022. DOI: `10.1007/978-3-031-06975-8_16`.
6. Z. Wang, T. Chen, Q. Dai, **Yinggang Guo**, Y. Chen, and H. Wei, "On-the-fly Quarantine Before Patches for N-day Kernel Vulnerabilities Are Available," in *ChinaSys'24 (Oral Presentation)*, 2024.

Journal

1. Z. Wang, **Yinggang Guo**, B. Zhong, Y. Chen, and Q. Zeng, "Dynamic Mitigation Solution Based on eBPF Against Kernel Heap Vulnerabilities," *JOS: Journal of Software*, 2023. DOI: `10.13328/j.cnki.jos.006923`.

Skills

Academic Research
Excellent at thinking and analyzing the logic behind problems, discovering and presenting new insights, and willing to communicate and collaborate.

Operating System
Solid foundation in Linux kernel; familiar with hardware features such as Intel PKU/PKS, WP, SMAP, and their application in system isolation.

Formal Modeling
Familiar with model-driven security analysis; skilled in B-method, and experienced in model checking using ProB.

Program Analysis
Master static analysis based on LLVM and various dynamic analysis techniques to analyze kernel data flow and control flow.

Teaching Experience

2022 Spring **Introduction to the Software Industry** as TA for undergraduates and graduates.

2020 Summer **Assembly Programming** as TA for undergraduates.

Projects

Kernel Compartmentalization
Secure, Scalable, and Efficient Kernel Compartmentalization based on the principle of least privilege. With **PKS-based bi-directional isolation**, a novel in-kernel monitor enforces multiple important security invariants, including data integrity, execute-only memory, and compartment interface integrity. Carefully designed switch gates and locality-aware address space switching efficiently support unlimited compartments. Extensive evaluations show that we can effectively prevent attackers from compromising the kernel through various types of vulnerabilities. Automatically compartmentalizing 160 LKMs incurs an average performance overhead of only 2.44% for real-world applications.

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

Yinggang Guo
Last update: 2024-08-31