郭迎港

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

研究兴趣

操作系统内核安全是我主要的研究方向，包括内核特权分离和内核模块分隔化。研究项目基于最小特权原则增强内核安全，通过形式化建模分析各种特权分离方案的安全效果，并利用新的硬件特性结合程序分析技术实现内核模块的安全高效分隔化，限制内核漏洞的影响。

教育背景

2019 – 2025 **博士, 南京大学** 计算机软件新技术国家重点实验室
研究方向: 操作系统安全，形式化分析
导师: 曾庆凯教授

2023 – 2024 **学术交流, University of Minnesota** Dept. of Computer Science & Engineering
研究方向: 内核模块分隔化
导师: Prof. Kangjie Lu

2015 – 2019 **本科，南开大学** 软件学院 优秀毕业生
研究方向: 控制流完整性

助教经历

2022 春季学期 **软件产业概论**，本研共修课程助教

2020 夏季学期 **汇编程序设计**，本科生课程助教

论文

会议

1. **Yinggang Guo**, Z. Wang, W. Bai, K. Lu, & Q. Zeng. (2025). BULKHEAD: Secure, Scalable, and Efficient Kernel Compartmentalization with PKS. In *NDSS'25* ***(CCF-A major revision)***.

   摘要: 本文利用 Intel Memory Protection Keys for Supervisor（PKS）机制实现了安全、高效、可扩展的 Linux 内核分隔化。通过双向隔离，轻量、新颖的 in-kernel monitor 保障了数据完整性、仅执行内存（XOM）、模块接口完整性等安全不变式。精心设计的 switch gate 和基于 Address Space Identifier（ASID）的局部性感知的地址空间切换大大扩展了 PKS 可支持的分隔域数量。实验表明我们可以有效防止攻击者通过各类型漏洞攻陷内核，自动化分隔 160 个内核模块仅产生了平均 2.44% 的性能开销。

2. **Yinggang Guo**, Z. Wang, B. Zhong, & Q. Zeng. (2022). Formal Modeling and Security Analysis for Intra-level Privilege Separation. In *ACSAC'22* ***(CCF-B)***.

   摘要: 本文提出了 privilege-centric model (PCM)，对代表性的内核同层特权分离方案如 x86-64 架构下的 Nested Kernel 和 AArch64 架构下的 Hilps 进行形式化建模。基于 ProB 的模型检测分析验证了不同方案满足的安全属性，可用于发现安全缺陷并指导系统设计。

3. R. Sun, **Yinggang Guo**, Z. Wang, & Q. Zeng. (2023). AttnCall: Refining Indirect Call Targets in Binaries with Attention. In *ESORICS'23* ***(CCF-B)***.
   摘要: 本文提出了一种新颖的神经网络结构来利用注意力机制学习二进制文件中函数调用点和被调用点的上下文匹配关系，将二进制函数间接调用目标的识别精确率和召回率分别提高了 31.4% 和 5%。

4. Z. Wang, **Yinggang Guo**, Y. Chen, & Q. Zeng. (2023). ERA: 基于 eBPF 的内核堆漏洞动态缓解研究. In 中国 *linux* 内核开发者大会 *CLK'23*.

5. B. Zhong, Z. Wang, **Yinggang Guo**, & Q. Zeng. (2022). CryptKSP: A Kernel Stack Protection Model Based on AES-NI Hardware Feature. In *IFIP SEC'22* ***(CCF-C)***.
   摘要: 本文提出了基于 AES-NI 加密的内核栈机密性和完整性保护方案。

6. Z. Wang, T. Chen, Q. Dai, **Yinggang Guo**, Y. Chen, & H. Wei. (2024). On-the-fly Quarantine Before Patches for N-day Kernel Vulnerabilities Are Available. In *ChinaSys'24 (Oral Presentation)*.
   摘要: 本文提出了基于 eBPF 的即时隔离来快速响应 N-day 内核漏洞的威胁。

期刊

1. Z. Wang, **Yinggang Guo**, B. Zhong, Y. Chen, & Q. Zeng. (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)***.
   摘要: 本文提出了一种基于 eBPF 进行数据对象空间随机化的内核堆漏洞动态缓解框架，用于在漏洞修复时间窗口中降低安全风险。其为漏洞报告中涉及的数据对象分配随机地址，使得攻击者无法准确放置攻击负载，堆漏洞利用难以成功，同时仅对系统造成约 1% 的性能损耗和可以忽略不计的内存损耗。

技能

学术研究	善于思考并分析问题背后的逻辑，发现并提出新的见解，乐于沟通协作。
操作系统安全	掌握 Linux 内核编程，熟悉基于 Intel CPU 硬件机制和虚拟化的多种隔离方案。
形式化建模	掌握基于 B 方法的形式化建模，熟悉模型检测工具 ProB。
程序分析	掌握基于 LLVM 的静态分析和各种动态调试技巧，分析内核数据流和控制流。

郭迎港

最后更新: 2024-07-29