倪书楷

中国北京

国籍: 中国 | 性别: 男 | 2000.10 | 138-1228-3130 | nishukai@hotmail.com

个人介绍

本人毕业于布朗大学安全系统实验室，目前在国家实验室专注于操作系统安全研究，尤其在二进制分析和系统研发方面积累了深厚经验，曾获得 ESORICS2024 杰出论文奖。在 SysXCHG 项目中，我们利用 BPF 技术精细划分内核态与用户态权限边界，实现了在不牺牲系统性能的前提下显著提升安全防护水平，从而有效降低潜在漏洞风险。此外，我参与的针对 eBPF 的劫持攻击研究，通过全面剖析 JIT 编译器与验证器的潜在缺陷，并结合软件中断隔离机制（SFI）实施防御，取得了突破性成果。这些成果不仅为常规内核攻击提供了全新的防护思路，也已成功应用于开放欧拉、麒麟等操作系统及国内顶级手机厂商，显著提高了产品安全性和市场竞争力。

教育经历

布朗大学, 导师 Vasileios P. Kemerlis — *GPA 4.0/4.0 - 普罗维登斯, 罗德岛*

数据科学与系统内核安全, 硕士 — *09. 2022 - 05. 2024*

- 软件安全与攻防, 操作系统, CPU/GPU 并行科学计算, 深度学习…

密涅瓦大学 — *GPA 3.8/4.0(前 5%) - 世界各地*

计算科学 & 金融分析, 学士 — *09. 2018 - 05. 2022*

- (三学位毕业) 数据科学与统计, 应用程序开发, 金融策略
- 算法与数据结构, 线性优化, 机器学习, 应用开发, 会计学, 全球金融策略…

技术能力

技术栈 Linux 内核, eBPF, gcc/LLVM, Git, CUDA, OpenMP, GDB, Docker, LaTeX, AWS

开发 C, Python, HTML/CSS/JavaScript, SQL, TensorFlow/PyTorch, jQuery, React.js

语言 英文, 中文

项目经历

国家实验室 — *北京, 中国*

基于硬件特性的操作系统安全隔离加固 — *2024 - 至今*

- 深入剖析 LLVM 内部（如 Selection DAG），并针对 eBPF 进行架构相关的优化，有效提升系统效率和安全。
- 利用软件中断隔离机制（SFI）对 eBPF 实现内存聚合和指令插装，显著降低潜在漏洞风险，并提升运行性能。
- 对 eBPF 下的 JIT 编译器与验证器进行全面分析，成功通过漏洞注入验证常规内核的提权漏洞。
- 对 Null_blk 等 10 余款设备驱动进行漏洞注入测试，验证加固方案在多种应用场景下的可靠性，进一步巩固了系统安全边界。
- 系统性收集并分类 1086 个内核漏洞，总结漏洞特点，为制定针对性的防护策略提供了数据支撑，从而优化整体安全策略。
- 成果已成功应用于开放欧拉、麒麟等操作系统，并与多家国内顶级手机厂商合作集成，显著提升产品安全性和市场竞争力。

讲师 — *中国*

安全攻防讲座 — *2024 - 至今*

- 为包括科威特、阿尔及利亚等中外客户定制安全攻防讲座，切实提升客户安全意识和应急响应能力。
- 解析数据投毒和对抗样本攻击等技术，通过实战案例展示 AI 攻防方案。
- 解析代码混淆及脚本、二进制和文件的恶意软件技术，讲解 Cobalt Strike、x32dbg、IDA 等工具的实战应用。

布朗大学安全系统实验室 — *普罗维登斯, 美国*

SysXCHG: 一种灵活的内核 syscall 设计 (CCS2023) 及其他进行中的项目 — *2022 - 至今*

- 设计了 Log N 时间复杂度的 syscall 过滤器, 提高了 seccomp bpf 在项目内的运行效率
- 定制化编译 Linux 内核 6.0.8, 实现了 arity 过滤器并优化其效率
- 为带有 syscall 准则的二进制文件设计了高灵活度的 syscall handler, 提升内核效率和可用性

美国银行 — *夏洛特, 美国*

数据自动化与技术研发 — *05. 2023 - 08. 2023*

- 实现了流程化审计数据测试与覆盖, 节约近 25% 计算和分析时间
- 通过 Python 和 Alteryx 自动化数据呈现和分析的流程
- 开发并优化了大数据集的并行计算和处理, 减少项目周期和成本

Elle Investments — *纽约, 美国*

全栈网络开发与高带宽同步的实现 — *05. 2022 - 12. 2022*

- 设计并实现了底层高可用数据储存, 减少 20% 写入, 40% 读取时间和 45% 内存使用
- 识别并修复数个 SQL 注入漏洞, 重构项目前后端 PHP, JavaScript 代码逻辑
- 实现动态 HTTP 缓存机制, 提升服务器并发数近 1000 倍