徐少文

15011128926 xushaowen@iie.ac.cn github.com/duowen1
中国科学院大学，中国科学院信息工程研究所 网络空间安全 • 博士
1996 年 11 月 8 日 北京石景山区 https://duowen1.github.io/

教育背景

至今 2019.09	**中国科学院大学，网络空间安全学院** • 信息工程研究所，网络安全测评实验室 网络空间安全专业 • 博士（研究方向：云和虚拟化安全，导师：贾晓启）
2019.06 2015.09	**北京理工大学** • 信息与电子学院 信息对抗技术 • 学士

科研成果

- ***Log2Policy: An Approach to Generate Fine-Grained Access Control Rules for Microservices from Scratch*** (ACSAC 2023, CCF-B) 第一作者；
- ***ConMonitor: Lightweight Container Protection with Virtualization and VM Functions*** (SoCC, CCF-B，在投) 第一作者
- ***SEDSpec: Securing Emulated Devices by Enforcing Execution Specification*** (DSN 2024，CCF-B) 参与作者。
- **面向容器主机平台的轻量级攻击检测方法及装置（专利号：CN115495731A）**专利第二作者；
- **一种基于 *Master-Slave* 模式的移动设备操作系统虚拟内核安全框架（审批中）**专利参与作者。

实习经历

- **绿盟科技·星云实验室（云安全实验室）2021 年 1 月-3 月**
  - 编写脚本（Python），持续爬虫以获取最新发布的漏洞信息；
  - 利用 eBPF 和 Falco，通过深入研究漏洞的攻击模式，编写规则匹配漏洞利用特征，实现了多个容器逃逸漏洞的攻击检测，规则已并入到绿盟商业产品中；
  - 开发容器逃逸的漏洞自动化攻击套件（Go），实现环境探测、投递 EXP、清理攻击痕迹、植入后门。

项目经历

- **Log2Policy**：基于日志的微服务应用访问控制规则生成方法
  - 针对于微服务应用人工难以正确配置访问控制规则的问题，提出了一种基于微服务应用日志分析的访问控制规则生成方法，需要预处理、拓扑图生成、属性挖掘和规则优化四个步骤；
  - 为了应对微服务应用频繁升级的特性，将微服务应用的升级分为了四种类型，并且提出了 free namespace 的升级策略。
- **ConMonitor**: 基于 VMFUNC 的容器运行时安全保护方法
  - 向系统中引入一个轻量级的 Hypervisor，为每个容器分配独立的 EPT 页表，使得内核与容器的物理内存相互隔离；
  - 利用 CPU 的 VMFUNC 机制实现快速的上下文切换，优化系统的性能。
- **Hyper-Tool**：基于硬件辅助虚拟化的闭源操作系统漏洞挖掘系统研制
  - 负责基础设施构建，基于开源的 Ddimon，搭建实验平台的 Hypervisor（C++），开发 Windows

驱动程序，利用硬件虚拟化实现系统调用、线程切换、内存访问、内存分配和回收、驱动模块加载的监控功能。

- **LXC 加固**：多平台内置式主动防御系统研制
  - 开发 Linux 内核模块（C），对内核中的关键数据结构进行周期性的度量，包括系统调用列表、关键系统函数等。如果发现数据结构被篡改，则会产生日志信息。
- **虚拟化书籍配套实验设计**：为《系统虚拟化：原理实现和安全》的内存虚拟化章节设计了基于 VMFUNC 和气球模型的配套实验。
- **远控攻击套件**：开发 Windows 和 Linux 内核驱动，实现端口隐藏和键盘记录，开发木马程序实现反沙箱、反调试和反虚拟化。
- **Tiny-Container**：通过调用内核接口实现基本的容器引擎（C），目前已开源：`https://github.com/duowen1/container-from-scratch-in-c`。
- **Clipboard-Monitor**：实现对剪切板的读取和局域网内的同步。

竞赛

- **腾讯极客大赛** 排名：58/800
  - 对 Javascipt 代码进行解混淆，题目包括实现快速幂算法、解 JsFuck、反汇编 WebAssembly、解基于虚拟机的代码混淆等`https://github.com/duowen1/geektree`。
- **Hackergame** 最高排名：324/2381。

计算机技能

- **软件开发**：能够使用 C、C++、Python 和 Go 语言开发应用、使用 Qt 开发跨平台的 GUI 应用程序，掌握 git、make、cmake、GDB、Docker 的使用方法，能够开发 Windows 和 Linux 的内核驱动（内核模块），熟悉内核的编程规范；
- **云原生技术**：深入了解容器的运行原理、了解容器平台上的各种安全威胁，了解云原生相关框架（Kubernetes、Istio），了解微服务、Serverless 等云原生应用模式的原理；
- **软件调试**：能够利用 IDA 对应用程序进行静态分析，能够利用虚拟机结合 Windbg 或 GDB 调试内核；
- **Linux 内核与 CPU 硬件**：深入理解内核的任务管理、内存管理、中断/异常处理、系统调用、文件系统和虚拟化（KVM），熟悉内核的配置、编译和调试，掌握 ftrace、kprobe、Tracepoint 等多种内核追踪方法，熟悉 x86 的体系结构，深入理解硬件辅助虚拟化，能够进行 x86 架构下的底层开发；
- **人工智能**：了解基本的机器学习算法，对大模型主要的攻击手段和防御方法有所了解，深入了解大模型 API 插件相关知识；
- **隐私计算**：了解 Intel SGX 的运行原理，熟知 SGX 的优势和劣势，能够开发 SGX 应用。对 Intel TDX、ARM TrustZone 和 CCA 有基本的了解。

获奖情况

- 2023 年获博士研究生国家奖学金；
- 中国科学院大学三好学生荣誉称号（2020-2021、2021-2022、2023-2024 学年）；
- 中国科学院信息工程研究所 2023 年度所长优秀奖。

其他技能

- 通过应用四六级、托福 98，能够流畅阅读英文文献，进行英语写作和 Presentation；
- 擅长沟通和团队合作，曾担任过子项目的负责人，具有较多报告撰写经验；
- 熟练使用 Office 办公软件，能够利用大模型或者开发小工具以提高工作效率。