随着网络空间安全的逐步发展以及对个人隐私的逐步重视，这几年略微降温的内核编程在个人隐私保护以及防泄密等领域渐渐升温，内核编程即将迎来第二春，而这本书不失为各位读者把握住这一技术潮流的最有利武器。

最后，在有幸作序之余，祝愿这本书能有更多的读者，能得到更多的认可，能发挥更多的作用，希望这本书能成为国内 Windows 内核编程领域的经典著作。

任晓珲
十五派信息安全教育创始人
《黑客免杀攻防》作者
黑客反病毒组织创始人
2020 年 2 月

前　言

Windows 是当前主流的闭源操作系统，从第一个 NT 内核的 Windows 2000 至今，已经有 20 年左右的历史。在这漫长的 20 年内，为了满足日益变化的业务需求，以及应对不断升级的安全挑战，Windows 操作系统内核一直不断升级与完善，其主要表现是内核中增加了新的逻辑模块与安全机制，其中最为典型的是 64 位的 Windows 操作系统内核对比 32 位内核增加了“Patch Guard”模块，这个模块的主要作用是检查内核是否被第三方内核模块“污染”，目的是防止病毒木马使用内核挂钩或劫持的技术篡改内核。新的安全机制往往会对安全开发者带来一定的影响，其原因是一些软件过度依赖系统未公开的底层技术，而正确的做法是开发者需紧密依赖系统提供的公开机制，利用可利用的机制完成相同的功能，这要求开发者对整个 Windows 内核机制有深入的理解。作者编写本书的目的之一，正是希望读者能对 Windows 内核有更全面、更深入的认识。

本书的前身是《Windows 内核编程与驱动开发》，本书在前者的基础上，删除了部分过时的章节，重写了大部分基础章节并新增了部分当前较为热门的技术，同时为了使本书内容更为聚焦，删除了与 Windows 内核关联性不强的内容。

本书面向的人群主要有以下几类。

- 有一定 C 语言基础，有兴趣了解 Windows 内核的读者。
- 有一定 C 语言基础，并且希望从事 Windows 内核开发的读者。
- 有一定基础的 Windows 内核开发者，有意愿进一步提高的读者。

本书共分为三篇。第一篇为基础篇（第 1 章～第 6 章），从初学者的角度出发，介绍 Windows 内核的基本概念、开发环境的搭建、系统机制以及内核编程的技巧。第 1 章与第 2 章是本书最为基础的部分，介绍了内核编程的基本概念与开发环境搭建，初学者应该首先学习这部分内容。第 3～第 5 章重点介绍了系统的常用机制，这些机制的使用会贯穿本书所有章节，掌握这些常用机制是内核开发者最基本的要求。第 6 章介绍了内核编程的注意事项与技巧，这些注意事项与技巧可以帮助初学者少走弯路，快速入门。

第二篇为过滤篇（第 7 章～第 18 章），是本书的核心内容，由易到难详细介绍了 Windows 系统的过滤机制。首先以最简单的串口过滤驱动开始，剖析了一个过滤驱动的最基本要素，然后分别介绍了键盘过滤、磁盘过滤、文件过滤以及网络过滤。对于网络过滤，本篇从不同的网络层次与角度介绍了 TDI、WFP 以及 NDIS 等机制。本篇内容涵盖了目前 Windows 系统绝大部分主流的过滤技术。

第三篇为应用篇（第 19 章～第 23 章），结合前两篇的知识点，本篇综合介绍了 Windows 安全领域所需的其他技术，通过对本篇的学习，读者将会发现安全技术并不局限于系统提供的现成机制。本篇选取了目前主流安全软件所使用到的典型技术，深入浅出，首先介绍了 CPU 的基本知识点，然后基于上述知识点，第 20 章重点介绍了 Windows 下的挂钩技术，挂钩技术常被用于安全软件的检测、审计、拦截等技术；第 22 章和第 23 章从守护的角度，为读者介绍了自我保护技术。

笔者拥有十余年的 Windows 开发经验，主导过数据安全、主机安全、服务器安全等项目，涉及 To C（面向消费者群体）和 To B（面向企业用户群体）行业，深知 Windows 内核的复杂性，由于行业的特殊环境，To C 和 To B 的内核技术方案选型不尽相同，因为不同的用户群体，其主机上软件存在参差不齐的同类安全软件，安全软件之间也存在大量的兼容性问题，这些问题的引入使得原本并不简单的内核编程更为复杂化。记得有很多读者问过我一个相同的问题：如何编写一个稳定的内核模块。这个问题其实没有标准答案，以笔者的经验来看，读者首先应该养成良好的编程习惯，然后深入理解系统的各种安全机制以及拦截方法，在编写代码时，请思考如下几个问题：①这句代码是否会被其他软件拦截导致失败；②这句代码是否会触发一些第三方的回调函数；③这句代码失败后应该怎么处理。本书在为读者介绍技术的同时，也为读者介绍了笔者的内核开发心得体会与技巧，希望这些体会与技巧可以为读者带来更多的思考。内核编程类似于武林秘籍的内功修炼，需要时间沉淀，并非一蹴而就，请读者赋予更多的耐心，“成功之道，贵在坚持”。

写作是一项工作量巨大而繁杂的工作，而对于技术书籍来说更是如此。由于我个人工作的缘故，写作只能在晚上或周末进行，有时为了整章内容的思路连贯而需要挑灯夜战，通宵达旦。一路走来，感谢我的父母、妻子和女儿，在每天有限的时间里，我需要投入更多的时间精力专注在写作上而缺少对他们的陪伴，尤其是我的女儿淇淇，在深感愧疚的同时，也感谢他们的理解与支持。

感谢我的挚友黄瀚，在本书写作过程中一直支持我，并为我提供了大量的技术性资源。感谢电子工业出版社的李冰老师和冯琦老师，她们的编辑工作确保了书本所有文字内容严谨与通畅。

感谢“安全圈”内朋友们的支持，尤其感谢数篷科技的科学家吴烨、CTO 杨一飞以及架构师王柏达，他们在工作中为我提供大量的帮助。感谢上一本书籍热心的读者，他们反馈的问题更好地完善了本书的内容。

最后，希望本书能为“安全圈”内的读者或者即将进入“安全圈”的读者带来更大的收获。

陈铭霖

2020 年 1 月于深圳

本书的作者和贡献者

本书的前身是《Windows 内核安全与驱动开发》，除了直接编写本书的作者，还有业内技术人士协同编写了部分章节，所有作者一并介绍如下。

谭文，网名楚狂人，已有十七年客户端安全软件开发经验。先后在 NEC、英特尔亚太研发有限公司、腾讯科技任职。曾从事过企业安全软件、x86 版 Android 的 houdini 项目、腾讯电脑管家、腾讯游戏安全等开发工作。对 Windows 内核有深入研究，现任腾讯科技游戏安全团队驱动程序开发负责人，专家工程师。指导了本书的主题思想，编写了核心过滤章节，并审核了所有新章节。

陈铭霖，现任职数篷科技终端安全负责人，负责终端安全开发。曾任腾讯科技高级工程师，主导腾讯电脑管家客户端安全项目；深信服科技 Windows 架构师，以及虚拟化产品架构师。有十余年终端安全开发经验，覆盖 To C、To B 及 To G 行业，具有千万级 DAU 安全产品的研发经验。主导了全书内容，重写了大部分章节，以及新增了部分章节。

张佩，Windows 驱动开发技术专家，长期从事声卡、显卡等硬件驱动程序的开发、调试工作。目前在英特尔亚太研发有限公司平板电脑相关部门工作。曾著有《竹林蹊径——深入浅出 Windows 驱动开发》一书。为本书贡献了若干个网络驱动相关的章节。

杨潇，曾任 Windows 客户端安全工程师，先后在上海贝尔和北京 Comodo 工作。后来离职创业，目前为西安一家医疗科技公司的 CEO。编写了本书“磁盘驱动”相关章节。

邵坚磊，网名 wowocock，业内著名的 Windows 安全技术专家。长期从事 Windows 安全相关的内核开发工作。目前在奇虎 360 任职。编写了本书部分章节并提供了部分代码实例。

卢冠豪，中国台湾人。毕业于辅仁大学资讯工程学系。长期从事 C、C++、网络与通信程序设计工作，参与过“端点安全”“资产管理”“网络流量分析”等项目的开发与维护，擅长 Windows 项目开发。编写了本书“文件系统微端口过滤”一章。

本书读者反馈的 QQ 群是 4088102，想了解更多信息也可以关注微信公众号：终端安全编程。

特别致谢

在本书的著作过程中，获得了安全界内热心朋友们的鼎力支持，他们的专业知识能力分布在国内不同的安全领域，为本书的基础定位、技术重点以及应用方向给出了科学的优化性建议。下面是为本书提供过帮助的专家们。

任晓珲（A1Pass），十五派信息安全教育 CEO，《黑客免杀攻防》作者，一位具有远大理想抱负的技术专家，笔者的挚友，他的价值观深深影响着笔者，受邀为本书作序，并且审阅了本书的主体脉络，结合当前行业形势为本书定位给出了宝贵的建议。

李常坤，奇安信技术总监，审阅了全书的主体脉络，为本书的技术构成给出了宝贵的建议。

黄瀚（EvilKnight），安全技术专家，笔者的挚友，在本书最开始进行技术选型时提供了大量的安全人脉资源，使本书的技术选型可以很好地满足行业内的不同需要。在本书编写的后期，审阅了本书的主要章节，提出了很多宝贵的建议。

杨一飞，数篷科技 CTO，百度前安全专家，笔者工作中的伙伴，生活上的挚友，行事低调却对技术有着狂热追求，在工作中为笔者提供了大量的帮助以及先进的技术理念，部分先进理念提炼后也被编写到本书中。

丰生强（@非虫），《Android 软件安全与逆向分析》、《macOS 软件安全与逆向分析》书籍作者，审阅了本书的主要章节，站在跨纬度的系统角度为本书给出了宝贵的意见。

胡训国，准动网络科技首席技术专家，前腾讯高级安全工程师，审阅了本书第三篇，帮忙勘正内容中的一些错误。

祁伟，华为终端安全专家，腾讯前高级安全工程师，审阅了本书的第一篇，帮忙勘正了内容中的一些错误。

王淙，Windows 内核驱动专家，审阅了本书第二篇的部分章节，帮忙勘正了内容中的一些错误。

邹冠群，资深软件安全专家，为本书的技术细节提供了部分参考资料。

张天郁，数篷科技 Windows 驱动专家，上海 2345 前内核高级工程师，受邀帮忙整理了本书的部分代码，以及更正了代码中的部分错误。

周子淇，软件安全专家，为本书的技术细节提供了部分参考资料。

丁健海，高级安全研究员，软件安全专家，为本书的技术细节提供了部分参考资料。

目　录

第 1 篇　基础篇