<<Windows PE权威指南>>

图书基本信息

书名：<<Windows PE权威指南>>

13位ISBN编号：9787111354185

10位ISBN编号：7111354184

出版时间：2011-10

出版时间：机械工业出版社华章公司

作者：戚利

前言

1988年11月，微软开始着手Windows NT的开发工作。
当时微软聘请了一组来自DEC公司且由Dave Cutler领导的开发人员。
正因为如此，NT操作系统的许多设计元素均借鉴了DEC在VMS和RSX-11上的前期经验，其中就包括目前Windows操作系统家族系列一直使用的核心文件格式PE/COFF。
1993年7月27日，Windows NT产品线的第一代产品NT 3.1问世。
该系统初次使用了PE格式作为操作系统的可执行文件格式。
同年，微软将该格式提交给工具接口标准委员会（Tool Interface Standard，TIS）并被获准。
随后，微软在不同版本的Windows操作系统中一直使用这种格式组织其核心可执行文件。
其间曾发布了多个PE/COFF版本，目前最新版本是2010年9月21日发布的8.2版。
微软采用术语“Portable Executable”来定义这个可执行文件格式，初衷是希望能开发一个在所有Windows平台上和所有CPU上都可执行的通用文件格式。
从目前的使用状况来看，这个目标已经基本实现。
该格式跨越了Windows操作系统的多个版本，从最初的NT和9x系列，到Windows XP/2000/Vista、Windows CE和目前流行的Windows 7。
作为一个被实践验证了的成熟而又稳定的核心文件格式，只要微软不放弃目前操作系统的内核，该格式势必会和操作系统长期共存。
Windows操作系统在市场上的巨大成功与PE文件格式的相对开放引起了广大计算机编程人员的兴趣。
通过对PE格式的理解，程序员不仅可以了解操作系统加载可执行文件的过程，还可以学习到操作系统对进程和内存进行管理的相关知识。
同时，通过一些技术手段，对PE文件实施变形或打补丁，还可以实现各种不同的应用，如汉化、加密解密、计算机安全、PE病毒等。
本书旨在对PE文件格式进行全面而深入的介绍，通过图示、分析和实例等帮助读者全面了解和掌握PE文件格式，最终达到能通过编程工具灵活地对PE文件进行编程，解决各种与PE文件格式有关的问题的目的。
本书适合的读者　　本书适合想详细了解Windows PE文件结构的人、想深入理解Windows系统进程管理及运作机制的人，以及计算机安全领域的初学者和对程序字节码感兴趣的人。
具体包括：　　初级水平的计算机安全爱好者　　对逆向工程、汉化、加密解密、病毒、黑客技术感兴趣的读者　　想提高MASM32编程技术的开发人员　　开设计算机安全课程院校的学生和老师
本书内容特色　　Windows操作系统是迄今为止最优秀的操作系统之一，而PE则是Windows操作系统中的核心文件格式。
本书以独特的视角（字节码），展开了对Windows PE文件格式的研究，并在充分理解PE文件格式的基础上，使用4种不同的方法对PE文件进行补丁，以实现各种不同的应用。
在基础理论方面，本书涉及诸多与Windows操作系统内部机制相关的知识，如Windows进程和线程管理、用户模式和内核模式下的Windows SEH异常处理、Windows内存管理与进程虚拟地址空间管理等。
在程序设计方面，本书涉及程序栈、重定位、线程本地存储、代码覆盖、动态加载、延迟导入、静态补丁等技术，并详细讲解了典型实例程序的编写思路及编码实现，这些实例包括：万能补丁码、EXE捆绑器、自动化安装工具、EXE加密、EXE加锁器、PE病毒提示器、网络文件下载器、PE在线自动升级程序、PE反病毒等。
全书共分三大部分：第一部分为PE的原理和基础，全面介绍了PE文件格式的基础技术；第二部分为PE进阶，主要讲解了PE文件变形和静态补丁技术；第三部分为PE的应用案例，主要讲解了如何通过对PE文件实施补丁程序来实现几种典型的应用。
以下是各章节的大致内容：　　第1章介绍了学习本书所需要的软件开发环境，以及相关辅助软件的使用方法，并开发了第一个基于MASM32的汇编程序，通过字节码阅读器初步认识本书中的主人公PE

文件。
在本章中，大家将学习到汇编程序从编写到编译、链接、执行的整个过程，了解并掌握汇编程序的调试方法，能对PE文件有一个初步的了解。

第2章介绍了3个常用的PE小工具的编写方法，它们分别是PEDump、PEInfo和PEComp，即PE十六进制字节查看器、PE结构分析器、PE文件比较器。

第3～10章是基础理论部分的重点，主要讲述了PE的结构。
其中第3章主要讲述了PE的文件头部分；第4～10章根据数据目录中数据的分类对各类别数据进行了从理论到实践的详细阐述，这些数据主要包括：导入表、导出表、资源表、重定位表、加载配置信息、线程局部存储（TLS）信息、延迟导入信息、绑定导入信息、IAT等。

<<Windows PE权威指南>>

内容概要

内容全面，详尽地剖析了Windows
PE文件格式的原理及其编程技术，涉及安全领域的各个方面和Windows系统的进程管理和底层机制；实战性强，以案例驱动的方式讲解了Windows
PE文件格式在加密与解密、软件汉化、逆向工程、反病毒等安全领域的应用，不仅每个知识点都配有小案例，而且还有多个完整的商业案例。

戚利编著的《Windows
PE权威指南》共分为三大部分：第一部分简单介绍了学习本书需要搭建的工作环境和必须具备的工具，深入分析了PE文件头、导入表、导出表、重定位表、资源表、延迟导入表、线程局部存储、加载配置信息等核心技术的概念、原理及其编程方法，有针对性地讲解了程序设计中的重定位、程序堆栈、动态加载等；第二部分讨论了PE头部的变形技术及静态附加补丁的技术，其中静态附加补丁技术重点讲解了如何在空闲空间、间隙、新节、最后一节四种情况下打补丁和进行编码的方法；第三部分精心编写了多个大型而完整的PE应用案例，以PE补丁作为重要手段，通过对目标PE文件实施不同的补丁内容来实现不同的应用，详细展示了EXE捆绑器、软件安装自动化、EXE加锁器、EXE加密、PE病毒提示器以及PE解毒的实现过程和方法。

《Windows
PE权威指南》不仅适合想深入理解Windows系统进程管理和运作机制的读者，而且还适合从事加密与解密、软件汉化、逆向工程、反病毒工作的安全工作者。
此外，它还适合想全面了解Windows
PE文件结构和对程序字节码感兴趣的读者。

作者简介

戚利，资深安全技术专家和软件开发工程师，对Windows PE、Windows内核、计算机网络安全、协议分析和病毒技术有较为深入的研究，实践经验丰富。
擅长汇编语言和Java技术，曾自主开发了一个RMI框架。
活跃于国内著名的安全论坛看雪学院，乐于与大家分享自己的心得和体会，且有较高的知名度。
此外，教学(副教授)经验也十分丰富，对读者的学习习惯和认知方式有一定的认识，这一点在本书的写作方式上得到了体现。

<<Windows PE权威指南>>

书籍目录

章节摘录

媒体关注与评论

本书内容针对性很强，学术研究和实践操作并重，不但适合计算机安全领域的初学者，对大专院校相关专业的学生也有很好的指导作用。
本书表述方式生动准确，理论与实践并重，通过本书，读者既能很好地了解PE格式，又能在实际工作和研究过程中运用这些知识。
因此，在本书付梓之际，感谢作者的辛勤付出，希望读者能够通过本书获得更多的收益！
——段钢看雪软件安全网站（WWW.pediy.com）创始人内容全面，全书围绕PE文件格式展开，不仅讲解了PE文件格式的原理和与之相关的编程技术和技巧，还以实例的方式讲解了PE文件格式在加密与解密、软件汉化、逆向工程、反病毒等安全领域的应用。
注重实践。
理论与案例相结合，不仅在各个知识点都辅有用以阐述理论的案例，而且还专门围绕PE的应用编写了多个具有商业价值的实用案例，这些案例相对完整且具有可扩展性和启发性。
强烈推荐！
——黑客反病毒组织（WWW.hackav.com）对于计算机领域的安全工作者而言，无论你是从事加密与解密、软件汉化相关的工作，还是从事逆向工程、反病毒相关的工作，都十分有必要系统而全面地掌握PE文件格式的原理和编程技术。
本书内容全面，从原理到应用，涵盖了PE文件格式的方方面面；实战性强，不仅为每个知识点配备了便于读者理解的小案例，还提供了几个大型的商业案例：结构清晰，语言通俗易懂，可读性较强。
十分难得！
——51CT0（WWW.51cto.com）

编辑推荐

《Windows PE权威指南》内容全面，详尽地剖析了Windows PE文件格式的原理及其编程技术，实践性强，以案例驱动的方式讲解了Windows PE文件格式在加密与解密、软件汉化、逆向工程、反病毒等安全领域的应用。
如果你是一位Windows内核研究者或系统级开发工程师，那么通过PE文件格式来理解windows的系统进程管理和运作机制会是一种很好的途径。
如果你是一位商业软件开发者，如何防止你的软件被反编译是必须要考虑的问题，最简单的办法就是对PE文件进行加密。
如果你是一位从事软件汉化的工程师，你必须对PE文件格式中拟汉化的资源的组织方式了如指掌。
如果你是一位反病毒工程师，除了要掌握各种病毒使用的基本技术外，还必须了解感染PE文件的病毒所采用的基本方法，以便能从容应对各种层出不穷的PE病毒。
如果你是一位有一定基础的计算机领域的安全工作者，那么系统地学习一JPE文件格式是你的必修课。
如果你的工作领域或兴趣与上述任何一个方面相关，《Windows PE权威指南》应该都能给你详尽的指导和帮助。

版权说明