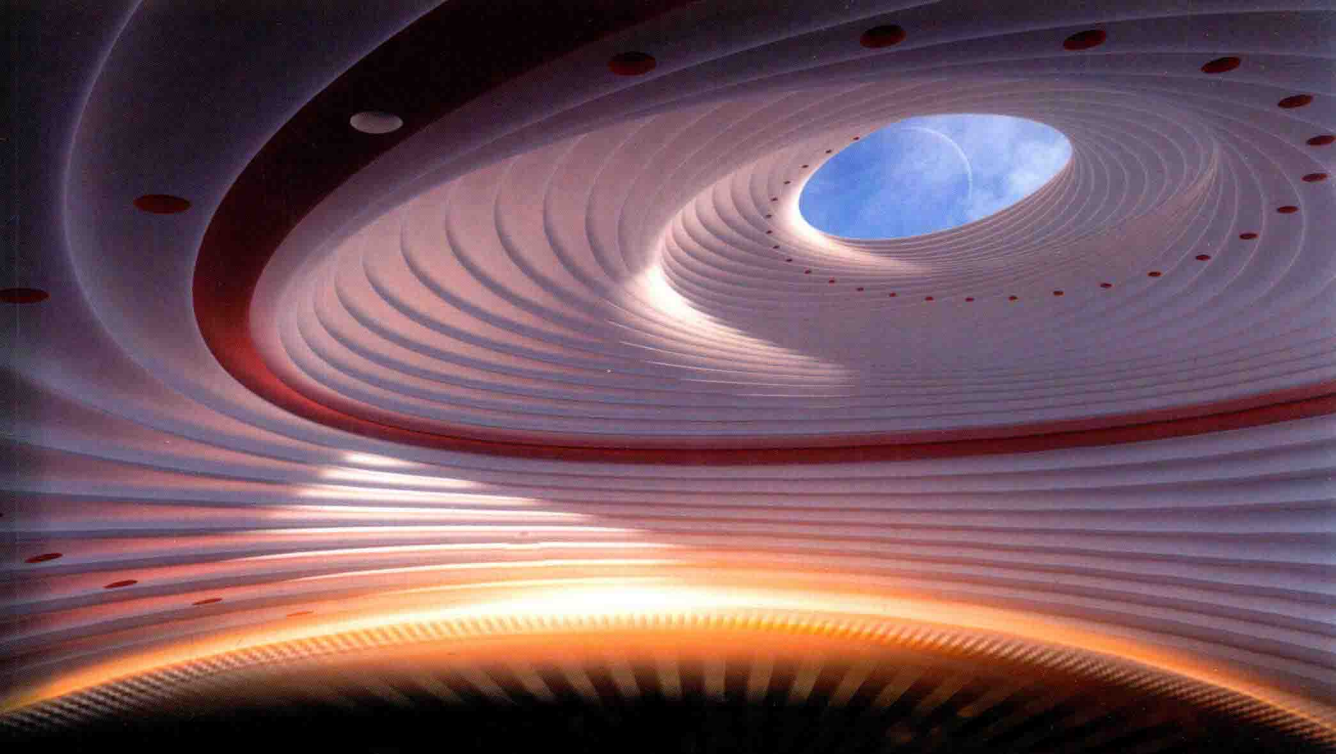

# Rootkit
# 隐遁攻击技术及其防范

The Rootkit Evasion Technology:
Attack and Prevention

张 瑜 ◎著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

# Rootkit 隐遁攻击技术及其防范

张　瑜◎著


電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

## 内 容 简 介

本书系统地论述了Rootkit隐遁攻击的概念、原理、应用技术及检测取证。首先，简要回顾了Rootkit的由来、定义、原理、类型及其演化。其次，阐述了Rootkit技术的基础理论，包括硬件系统、软件系统，以及Windows内核驱动程序设计。然后，重点探讨了Rootkit攻击技术的具体类型及其实现，包括用户层Rootkit、内核层Rootkit、固件Rootkit及硬件Rootkit。最后，从防御的角度讨论了Rootkit检测与取证技术，以及Rootkit未来的发展趋势。

本书取材新颖，聚焦前沿，内容丰富，可作为IT和安全专业人士的研究指导用书，同时也适合作为高等学校计算机安全专业本科、研究生的参考教材。



**图书在版编目（CIP）数据**

Rootkit隐遁攻击技术及其防范 / 张瑜著. —北京：电子工业出版社，2017.1

ISBN 978-7-121-30618-1

Ⅰ. ①R… Ⅱ. ①张… Ⅲ. ①计算机病毒－防治 Ⅳ. ①TP309.5

中国版本图书馆CIP数据核字（2016）第304242号

策划编辑：秦绪军　朱雨萌

责任编辑：秦绪军

特约编辑：刘广钦　刘红涛

印　　刷：北京京科印刷有限公司

装　　订：北京京科印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路173信箱　　邮编：100036

开　　本：787×1092　1/16　印张：17.25　　字数：386千字

版　　次：2017 年 1 月第 1 版

印　　次：2017 年 1 月第 1 次印刷

定　　价：58.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）88254750。

# 前 言

社会信息化与网络泛在化已成为全球趋势。无处不在、如影相随的信息网络，极大地改变了人们的生产与生活方式，深刻地影响着社会发展的方方面面。网络和信息技术的加速渗透与深度应用，引发了人们对于网络空间安全的担忧。2014 年成立的中央网络安全和信息化领导小组，标志着网络空间安全问题已提升为国家战略。

近年来，网络攻击者（黑客）利用日益增强的网络依赖性和不断涌现的软件漏洞，通过隐匿恶意软件远程渗透、潜伏并控制目标网络系统，悄无声息地窃取敏感信息、实施网络犯罪并伺机发起网络攻击，获取政治、经济和军事利益，已造成了严重的网络安全威胁。

网络犯罪的趋利化，促使网络攻击者不断革新网络攻击理念，创新网络攻击方式，竭力占据网络攻防的技术优势。隐遁攻击（Evasion Attacks）就是在此背景下出现并迅速发展起来的一种恶意网络攻击新形态，具有极大的破坏力。所谓隐遁攻击，是指一种利用隐遁技术，通过伪装或修饰网络攻击痕迹，以规避、阻碍信息安全系统检测与取证的恶意网络攻击。攻击者对已被渗透的目标网络系统发动的隐遁攻击，犹如隐形战机在雷达未能有效探测的情况下发起的攻击，如入无人之境，令人束手无策，安全威胁极大。

在各类隐遁攻击方式中，Rootkit 隐遁攻击无疑最具威胁性，它钩挂系统服务，调用、篡改系统内核数据，寓攻击于无形之中，来无影去无踪，攻击威力极大。所谓 Rootkit 隐遁攻击，是指借助尖端的 Rootkit 技术来隐匿自身及其攻击痕迹，从而阻碍、规避取证分析的一种新型恶意网络攻击。其威胁性主要体现在两个方面：①通过钩挂系统服务调用以更改指令执行路径，致使传统的网络安全防御工具难以检测取证；②通过篡改系统内核数据，使其毫无察觉地潜伏于目标系统中多年，而用户对此却一无所知。

此类攻击案例不胜枚举，例如，2010 年著名的黑客大会（Black Hat）上，Barnaby Jack 利用 Rootkit 隐遁技术，使 ATM 机狂吐现金，震撼全场；2012 年波及全球的 Flame 攻击，造成多数国家机密资料失窃，攻击力极强；2013 年震惊世界的美国“棱镜计划”，隐秘渗透目标系统并植入恶意软件，实施暗中监控、窃取政情军情，并发起定向隐遁攻击，危害极大；2016 年乌克兰电网攻击事件，黑客利用隐遁攻击致使 30 座变电站停运，造成超过

23 万名居民陷入无电可用的困境。这些网络攻击案例表明，黑客早已利用顶尖的 Rootkit 隐遁技术，通过先期渗透并潜伏于目标网络系统中，窃取敏感信息、实施网络犯罪、发起悄无声息且破坏力巨大的隐遁攻击，已成为一种非常严重的网络安全威胁。

更为严重的是，为了规避、阻碍传统的磁盘文件系统取证分析，Rootkit 隐遁攻击已开始采用驻留内存、伪装内存等反取证对抗措施，造成无证可取、取得伪证等后果。主要体现在两个方面：①驻留内存的 Rootkit 隐遁攻击。此类攻击表现为：无磁盘文件，Rootkit 全部在内存中加载运行，目标机器关机后，实施攻击的文件映像自我删除、自动消失，致使无证可取。②伪装内存的 Rootkit 隐遁攻击。此类攻击表现为：即使有磁盘文件，但其在内存中运行后便实施内存视图伪装，以蒙混欺骗相关实时检测取证工具，致使取得伪证。因此，作为一种隐遁网络攻防的有力武器，Rootkit 及其防御技术已成为信息安全领域研究者所共同关注的热点。从 Rootkit 隐遁攻击的发展趋势来看，对 Rootkit 隐遁攻击进行深入研究与分析，已是大势所趋、势在必行。

然而，目前国内几乎没有关于 Rootkit 隐遁攻击及其防范全面系统的论述，也几乎没有一部专门阐述 Rootkit 隐遁攻击技术及防范的著作。在这种背景下，为了促成国内网络空间安全技术的研究，重视 Rootkit 隐遁攻击的理论指导作用和实践应用效用，笔者结合自己多年来在网络安全、恶意代码取证及免疫计算等领域的研究与体会，特编撰拙著，以期抛砖引玉。

本书全面翔实地介绍了 Rootkit 的起源、定义、演化发展、检测与取证分析，系统研究并总结了 Rootkit 隐遁攻击技术的内在机理，包括硬件系统基础、软件系统基础，以及 Windows 内核驱动程序设计等。并在此基础上，深入研究探讨了 Rootkit 隐遁攻击技术的不同类型与应用场景，包括用户层 Rootkit、内核层 Rootkit 和底层 Rootkit 等。然后，从防御的角度探究了 Rootkit 隐遁攻击的检测与取证分析方法。因此，本书所涉主题有矛有盾、攻防兼备。从矛的方面来说，Rootkit 隐遁攻击技术的研究，为网络空间进攻武器研发提供了研究思路；从盾的角度来说，Rootkit 防御技术的研究，为检测取证防御产品的研制提供了参考与借鉴。

全书分为 9 章。第 1 章为 Rootkit 概述，介绍了 Rootkit 的起源、定义和演化发展等；第 2 章讨论了 Rootkit 的硬件系统基础，介绍了保护模式及其执行环境、CPU 特权级、内存分段与分页，以及内存访问控制体系等；第 3 章讨论了 Rootkit 的软件系统基础，包括 Windows 设计原则、体系结构、分段与分页，以及系统服务调用机制等；第 4 章从程序设计的角度阐述了 Windows 内核驱动程序设计及相关概念、原理，为 Rootkit 设计开发提供支撑；第 5 章讨论了用户层 Rootkit 原理及相关技术实现；第 6 章介绍了内核层 Rootkit 原理及相关技术实现；第 7 章讨论了底层 Rootkit 的相关原理；第 8 章探讨了 Rootkit 防御技

术，包括 Rootkit 检测与取证分析方法，并结合笔者的工作提出了一些新的思路与观点；第 9 章为本书的结论部分，展望了 Rootkit 未来的发展方向与趋势。

本书的研究与撰写工作获得了国家自然科学基金（编号：61262077、61462025）、国家留学基金委、海南省重点研发计划项目（编号：ZDFY2016013）和海南师范大学学术专著出版基金等研究项目的资助。

本书从各种论文、书刊、期刊及网络中引用了大量资料，有的已在参考文献中列出，有的无法查证，在此谨向所有作者表示衷心的感谢！此外，衷心感谢美国 Sam Houston State University 的 Qingzhong Liu 博士，在笔者于 2013－2014 年在该校作访问学者期间，在生活和科研上给予了很大的支持与帮助！真诚感谢四川大学计算机学院的李涛教授的栽培与教诲！感谢海南师范大学信息学院的罗自强博士、曹均阔博士、刘晓文博士、何书前博士的支持与帮助！

作 者

2016 年 9 月

# 反侵权盗版声明

# 目 录

# 1 第1章 Rootkit概述

## 1.1 Rootkit的由来

近年来，网络攻击者（黑客）利用日益增强的网络依赖性和不断涌现的软件漏洞，通过隐遁技术远程渗透、潜伏并控制目标网络系统，悄无声息地窃取敏感信息、实施网络犯罪并伺机发起网络攻击，获取政治、经济和军事利益，已造成了严重的网络安全威胁[1]。据 *2016 Internet Security Threat Report*[2] 报道：全球50%的互联网用户遭受过网络攻击，中国有77%网民遭受过网络攻击，为全球第二大网络攻击受害国；全球因网络攻击造成了1130亿美元的经济损失，中国因网络攻击造成了370亿美元损失。另据IBM X-Force安全研究小组[3]针对2015年典型攻击情况的分析调查显示，近70%的网络攻击为未知（Unknown）原因的攻击。因此，有理由相信：隐遁攻击技术已被黑客广泛采用。

Rootkit就是在此背景下出现并迅速发展起来的一种隐遁网络攻击新技术[4]。Rootkit是一种通过修改操作系统内核或更改指令执行路径，来隐藏系统对象（包括文件、进程、驱动、注册表项、开放端口和网络连接等），以逃避或者规避标准系统机制的程序[5,6]。攻击者借助于Rootkit隐遁技术对已被渗透的目标网络系统发动的网络攻击，犹如隐形战机在雷达未能有效探测的情况下发起的攻击，如入无人之境，令人束手无策，安全威胁极大[7]。据 *McAfee Labs 2014 Threats Predictions*[8] 报告预测：网络攻击者将会使用更多的Rootkit隐遁攻击技术，以逃避检测与取证，获取更大的利益。

鉴于 Windows 系统的普及性，Windows Rootkit 已成为网络空间攻防双方的重点研究对象，本书主要讨论 Windows 系统中的 Rootkit 技术。

Windows 系统的 Rootkit 技术研究始于 1999 年 Greg Hoglund[9] 在著名黑客杂志 *Phrack* 上发表的 *A Real NT Rootkit*。该文作者创造性地提出了多项 Windows 系统内核隐遁技术，获得了信息安全社区的极大关注，同时也开启了 Windows 系统 Rootkit 技术研究的先河。之后，几乎每期 *Phrack* 都有与 Rootkit 相关的技术论文。此外，著名的黑客大会（Black Hat、Def Con 等）从 2005 年也开始了 Rootkit 技术讨论议题。

工业界和政府部门同样关注 Rootkit 技术研究与应用。日本索尼公司在 2005 年使用 Rootkit 技术保护其 BMG CD 版权，以防止光碟被非法复制 [10]。美国和以色列联合研制的采用了 Rootkit 隐遁技术的“震网病毒 Stuxnet”[11]，于 2010 年重创伊朗核电设施，严重滞后其核计划。2013 年震惊世界的美国“棱镜计划”[12]：隐秘渗透目标系统并植入采用 Rootkit 隐遁技术的恶意软件，实施暗中监控、窃取政情军情，并发起定向隐遁网络攻击。与此同时，Rootkit 检测防御工具也相继出现，譬如，Mark Russinovich 编写的 Rootkit Revealer，EP_X0FF 编写的 Rootkit Unhooker，Joanna Rutkowska 编写的 System Virginity Verifier，Linxer 开发的 PCHunter，Dmitry 开发的 Tuluka Kernel Inspector，GMER 研究团队开发的 GMER，F-Secure 公司的 Blacklight，McAfee 公司的 Rootkit Remover，Kaspersky 公司的 TDSSKiller，以及 Sophos 公司的 Anti-Rootkit 等。

国内对于 Rootkit 及其防御技术的关注和研究相对较早。中国科技大学 [13]、上海交通大学 [14,15]、电子科技大学 [16,17]、解放军信息工程大学 [18,19]、华中科技和北京大学 [20] 等高校已相继开展了 Rootkit 及其防御技术分析研究；相关的 Rootkit 检测工具主要有：潘剑锋开发的 IceSword，CardMagic 和 Wowocock 编写的 DarkSpy，以及 Linxer 开发的 PCHunter 等。

作为一种隐遁网络攻防的有力武器，Rootkit 及其防御技术已成为信息安全领域研究者所共同关注的热点。关于 Rootkit 研究综述已取得部分研究成果。譬如，Bravo 等 [21] 从 Rootkit 产生机制的角度综述了当前的 Rootkit 技术发展、分类及防御，主要侧重于 Linux 系统；Joy 等 [22] 从 Rootkit 防御机制方面综述了现今 Rootkit 检测技术的研究进展；Shields 等 [23] 从取证的视角综述了目前 Rootkit 技术研究进展；李文新等 [24] 综述了 Android 系统 Rootkit 的实现原理及检测方法。然而，目前国内详细而全面介绍 Windows 系统 Rootkit 机理与研究成果的学术专著少之又少。为了深入理解 Windows Rootkit 的机理和发展趋势，总体把握 Windows Rootkit 及其防御研究进展，并促进国内在该方向上的研究，探究并总结 Windows 系统 Rootkit 技术的新进展与新方法非常必要。

## 1.2　Rootkit 的定义

Rootkit 一词源于 UNIX 系统。在 UNIX 系统中，Root 是指拥有所有特权的管理员，而 Kit 是管理工具，因此，Rootkit 是指恶意获取管理员特权的工具。利用这些工具，可在管理员毫无察觉的情况下获取 UNIX 系统的访问权限。

对于 Windows Rootkit，尽管在名称上沿用了 UNIX 系统的 Rootkit，但在技术上则继承了 DOS 系统相关隐形病毒技术：拦截系统调用以隐匿恶意代码。最早出现的 Windows Rootkit-NT Rootkit，由美国著名信息安全专家 Hoglund 提出并编码实现，且对后来的 Rookit 研究产生了极大的影响。

Hoglund[9] 给出的定义如下：Windows Rootkit 是能够持久或可靠地、无法检测地存在于计算机上的一组程序和代码。俄罗斯著名的 Kaspersky 实验室反病毒专家 Shevchenko[25] 对 Windows Rootkit 的定义如下：它是一种通过使用隐形技术来隐藏系统对象（包括文件、进程、驱动、服务、注册表项、开放端口和网络连接等），以逃避或者规避标准系统机制的程序。微软著名安全专家 Mark Russinovich 给出的定义如下：一种将自身或其他对象隐藏起来，以躲过标准诊断、管理和安全软件查看的软件。Michael A. Davis 给出的定义如下：Rootkit 是能够长时间存在于计算机上或自动化信息系统上的未被发现的程序和代码集合。Bill Blunden 给出的定义如下：Rootkit 可以在机器上建立一个远程接口，该接口允许攻击者以一种难以察觉的方式（隐藏）对系统进行操纵（指挥与控制）和收集数据（侦察）。

尽管上述定义不尽相同，但都刻画出了 Windows Rootkit 的本质特征 [21,22]：①隐匿性；②持久性；③越权性。因此，从本质上分析，Rootkit 是破坏 Windows 系统内核数据结构及更改指令执行流程 [26,27] 的代码，Rootkit 可提供 3 种服务：①隐遁；②侦察；③控制。Rootkit 应由其所提供的服务而不是由其如何实现服务来定义的。

鉴于此，本书给出如下定义：Windows Rootkit 是一种越权执行的程序或代码，常以驱动模块加载至系统内核层或硬件层，拥有与系统内核相同或优先的权限，进而修改系统内核数据结构或改变指令执行流程，以隐匿相关对象、规避系统检测取证，并维持对被入侵系统的超级用户访问权限。

## 1.3　Rootkit 的原理

计算机系统是硬件系统与软件系统有机结合的复杂系统。硬件系统中的 CPU 借助于硬件环和特权指令进行访问控制，借助于 CPU 表和系统表来跟踪相关信息，利用分页与

地址转换机制来使用内存。软件系统中的操作系统则更加复杂，不仅涉及其体系结构，还牵涉如何基于 CPU 的硬件环来进行特权保护，以及如何利用 CPU 的分段、分页、虚拟存储机制来进行内存分配与管理。

面对复杂的计算机系统，需要首先解决两个问题：①如何化繁为简，将复杂系统简洁化；② Rootkit 的设计理念是什么，即 Rootkit 如何与计算机系统交互。下面将分别讨论。

### 1.3.1 计算机系统的抽象

作为一个哲学概念，抽象（Abstraction）是通过分析与综合的途径，运用概念在人脑中再现对象的质和本质的方法，分为质的抽象和本质的抽象。分析形成质的抽象，综合形成本质的抽象。作为科学体系出发点和人对事物完整的认识，只能是本质的抽象（具体的抽象）。

抽象是从众多的事物中抽取出共同的、本质性的特征，而舍弃其非本质的特征。要抽象，就必须进行比较，没有比较就无法找到在本质上共同的部分。共同特征是指那些能把一类事物与他类事物区分开来的特征，这些具有区分作用的特征又称本质特征。抽取事物的共同特征就是抽取事物的本质特征，舍弃非本质的特征。所以，抽象的过程也是一个裁剪的过程。在抽象时，异与同决定从什么角度上来抽象。抽象的角度取决于分析问题的目的。

在计算机科学中，抽象是简化复杂的现实问题的途径，它可以为具体问题找到最恰当的类定义，并且可以在最恰当的继承级别解释问题。它可以忽略一个主题中与当前目标无关的那些方面，以便更充分地注意与当前目标有关的方面。抽象并不打算了解全部问题，而只是选择其中的一部分，暂时不考虑其他部分细节，即抽象侧重于相关的细节和忽略不相关的细节。抽象作为识别基本行为和消除不相关的及烦琐的细节的过程，允许设计师专注于解决一个问题的有关细节而不考虑不相关的较低级别的细节。软件工程过程中的每一步都可以看做对软件解决方法的抽象层次的一次细化。在进行软件设计时，抽象与逐步求精、模块化密切相关，帮助定义软件结构中模块的实体，由抽象到具体地分析和构造出软件的层次结构，提高软件的可理解性。

抽象包括两个方面：①过程抽象；②数据抽象。可用 3 类图形表示：①层次结构图；②嵌套结构图；③树形结构图。

概括而言，“抽象”可包含以下几个含义。

- 展示事物概要结构。
- 隐藏具体细节以展示事物本质。

- 将复杂系统划分为较小的简单的子系统，并明确各子系统的功能职责。

计算机系统是一个复杂系统。对复杂事物进行分析的最佳方法是抽象分层。通过将系统划分为若干较小的模块并明确各模块之间的交互接口，采取化整为零的方式才能研究设计好复杂的计算机系统。只要多添加一个间接层，计算机科学就没有对此解决不了的问题[28]。

目前，在计算机系统中，有两类常用的抽象分层结构：①层次结构；②客户 / 服务器结构。所谓层次结构，就是将计算机系统的所有功能模块按功能的调用次序分别排列成若干层，各层之间的模块只能是单向依赖或单向调用关系。

层次结构的优点如下：

- 复杂问题局部化，增加系统的可读性。
- 层次之间的组织结构与依赖关系清晰化，增加系统的可靠性。
- 层次的增减简单化，增加系统的灵活性与可适应性。

客户 / 服务器结构是为适应网络环境应用而设计的。采用此类结构的软件系统由两大部分组成：①运行于核心态的内核；②运行于用户态并以客户 / 服务器方式运行的进程层。内核提供所有操作系统的基本操作，如线程调度、虚拟存储、消息传递、设备驱动，以及内核的原语操作集和中断处理等。

除内核之外，操作系统其他部分被分成若干个相对独立的进程，每个进程实现一组服务。此类服务进程可提供诸如系统功能、文件系统服务和网络服务等服务，检查客户是否提出要求服务的请求，并将相关结果返回给客户进程。客户进程与服务器进程之间的通信是通过互发消息来进行的。由于不同进程拥有不同的虚拟地址空间，所以，它们之间不能直接通信；而内核可被映射至每个进程的虚拟地址空间，它可操作所有进程通信，因此，不同进程之间的通信需借助于内核通过发消息的方式进行。

众所周知，基于冯 · 诺依曼体系的计算机系统可分为软件系统和硬件系统。在软件系统中，所有高级语言都以迭代或递归算法来处理数据，且所有语言均需翻译成更低级的机器语言才能执行或解释。在硬件系统中，所有物理机器均由逻辑门构成的组合或时序电路组成。因此，从软件和硬件的角度来看，计算机系统的分层如图 1-1 所示。


图 1-1　计算机系统的分层

从逻辑抽象层次来看，计算机系统自上至下可分为 7 层（见图 1-2）：①应用层；②高级语言层；③汇编层；④操作系统层；⑤指令集架构层；⑥微代码层；⑦逻辑门层。


图 1-2　计算机系统的层次结构

在计算机系统中，操作系统是一种复杂的大型软件。对复杂事物进行分析的最佳方法就是上述所讨论的抽象分层。通过将操作系统划分为若干较小的模块并明确各模块之间的交互接口，采取化整为零的方式才能研究设计好复杂的操作系统。

操作系统提供两个基本功能：①防止硬件被失控的软件滥用文件管理；②为软件提供统一的机制以访问硬件设备。操作系统通过 3 个抽象概念来实现这两个功能：①文件；②虚拟存储器；③进程。文件是对 I/O 设备的抽象表示，虚拟存储器是对主存和 I/O 设备的抽象表示，进程是对 CPU、主存和 I/O 设备的抽象表示。因此，从逻辑抽象的角度，操作系统提供的抽象如图 1-3 所示。

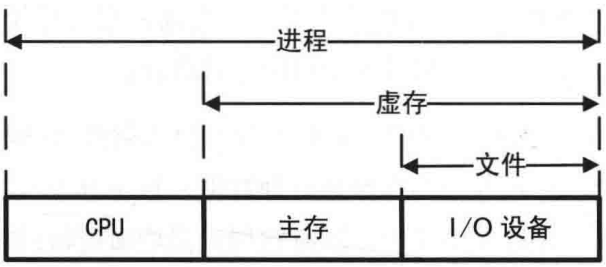


图 1-3　操作系统提供的抽象

在计算机系统中，上层系统的实现最终还是依靠底层的硬件系统支撑。而硬件系统的功能很大程度上依赖于 CPU。现代桌面系统的 CPU 提供了诸多硬件机制，主要包括物理内存分段和编址方式、CPU 寄存器、操作模式、地址扩展方法及访问控制等。CPU 除了跟踪环的信息之外，还需负责其他相关决策实施，如中断例程执行、线程切换等。要完成这些任务，CPU 必须知道这些例程的地址，这些地址通常存放在 CPU 相关表中。重