



信息安全国家重点实验室

信息安全丛书

Secure Operating System
Principle and Technology

安全操作系统 原理与技术

刘克龙 冯登国 石文昌 编著



科学出版社

www.sciencep.com

信息安全国家重点实验室信息安全丛书

安全操作系统原理与技术

刘克龙 冯登国 石文昌 编著

科学出版社

北京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。全书主要内容涵盖了安全操作系统的各个方面:安全操作系统的研究发展进程、安全需求与安全策略、安全模型、安全体系结构、安全操作系统的设计与实现、国外知名安全操作系统介绍、安全操作系统测评标准以及安全操作系统的应用场景等等。

本书可作为高等院校计算机、通信、信息安全等专业的教学参考书,也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

安全操作系统原理与技术/刘克龙,冯登国,石文昌
编著. —北京:科学出版社,2004
(信息安全国家重点实验室信息安全丛书/冯登国主编)
ISBN 7-03-013676-4

I. 安… I. ①刘…②冯…③石… II. 操作系
统-安全技术 N. TP316

中国版本图书馆 CIP 数据核字(2004)第 056185 号

策划编辑:鞠丽娜/责任编辑:马长芳
责任印制:吕春珉/封面设计:王 浩

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004年7月第一版 开本:B5(720×1000)
2004年7月第一次印刷 印张:24 3/4
印数:1—5 000 字数:481 000

定价:38.00 元

(如有印装质量问题,我社负责调换〈环伟〉)

《信息安全国家重点实验室信息安全丛书》编委会

顾问 蔡吉人 何德全 林永年 沈昌祥 周仲义

主编 冯登国

编委 (按姓氏拼音字母排序)

陈宝馨	陈克非	戴宗铎	杜虹	方滨兴
冯克勤	郭宝安	何良生	黄民强	荆继武
李大兴	林东岱	刘木兰	吕诚昭	吕述望
宁家骏	裴定一	卿斯汉	曲成义	王煦法
王育民	肖国镇	杨义先	赵战生	张焕国

序 言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破,形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地,也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花,如雨后春笋,在华夏沃土上竞相开放,炎黄子孙们,在经历了几百年的苦难历程后,在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握,非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面,就会不经意地释放出它危害人类的一面。

生产力的发展,为社会创造出许多新的使用价值。但是,工具的不完善,会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样,由于人类认识真理和实践真理的客观局限性,存在许多不完善的地方,从而形成信息系统的漏洞,造成系统的脆弱性,在人们驾御技能不足的情况下,损害着人们自身的利益。

世界未到大同时,社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力,在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性,运用其“暴智”来散布计算机病毒,制造拒绝服务的事端,甚至侵入他人的系统,盗窃资源、资产,以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展,信息安全成为全社会的需求,信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定,也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现,取决于信息安全是否得以保障。什么是信息安全?怎样才能保障信息安全?这些问题都是严肃的科学和技术问题。面对人机结合,非线性、智能化的复杂信息巨系统,我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候,就盲目乐观地向世人宣称,我们拥有了全面的解决方案;我们也不能因为面对各种麻烦,就灰头鼠脸,自暴自弃,我们需要的是具有革命的乐观主义精神,坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的,今天对信息安全的认识,就经历了一个从保密到保护,又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的,它涉及到人、社会和技术,因此,仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看,只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段,才能取得良好的效果。

为了推动我国信息化发展的进程,信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中,我们既注重学术水平,又注意其实用价值。本丛书从信息安全保障体系,操作系统安全,数据库安全,网络安全,无线网络安全,网络攻击,密码技术,PKI 技术,信息隐藏,安全协议,安全事件应急响应,量子密码通信等多个角度,分析和总结信息安全的科学问题以及信息安全保障的理论与技术,因此,这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中,以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获,从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的,今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言,它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们共同努力,不断地深化自己的研究,借鉴国外先进的科学技术,结合国情,与时俱进地推出信息安全保障的新理论、新办法和新手段,用我们的智慧保卫我们的信息疆土,使我们的信息家园尽量祥和安宁。

限于作者的水平,本丛书难免存在不足之处,敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前 言

纵观计算机的发展历史,早期的计算机使用者一般集中在大学校园、研究所等学术研究气氛浓郁的环境中,安全自然不是考虑的首要问题,功能全面和使用便捷才是人们最关心的。这一观念沿袭至今。然而,在飞速发展的 Internet 计算环境中,我们处于一个两难的境地,一方面现实世界依赖计算机系统的程度越来越高,另一方面计算机系统的安全性问题越来越突出。原先彼此信任的前提条件已经不再成立,不法分子利用网络的掩护打家劫舍、肆意妄为,系统安全管理员则在“猫和老鼠”的游戏中应接不暇、疲于奔命。

近些年来,随着互联网攻击事件的日益猖獗,国内外信息安全专家希望找到一种更为行之有效的方法来解决黑客攻击这一令人头疼的问题。正是基于此,人们从疲于奔命的对软件打补丁的思维桎梏中解脱出来,尝试通过增强操作系统的安全性来达到从源头上扼制黑客攻击的可能性。因为操作系统是整个计算机系统的基础,它管理计算机资源、控制整个系统的运行、直接和硬件打交道,并为用户提供接口。无论是数据库系统还是应用软件系统,它们都是建立在操作系统之上的,都是通过操作系统来完成对系统中信息的存取和处理。在网络环境中,网络的安全可信性的基础是连网各主机系统的安全可信性,而主机系统的安全性又依赖于其操作系统的安全性。因此,可以认为操作系统安全是整个计算机系统安全的必要条件。

本书共分 10 章。第 1 章为绪论,重点讲述当前快速发展的信息化网络环境下存在的安全风险和安全威胁,并简要阐述操作系统安全性的重要意义;第 2 章为主流操作系统的安全机制,讲述目前两种流行的操作系统:Windows 系统与 Linux 操作系统的主要安全机制;第 3 章为安全操作系统研究的发展,讲述国内外对安全操作系统的研究的发展进程;第 4 章为安全需求与安全策略,简要描述安全需求与安全策略的方方面面;第 5 章为操作系统安全体系结构,讲述操作系统的安全体系结构的含义及类型以及安全体系结构的设计基本原则,并重点介绍了 Flask 体系结构;第 6 章为形式化方法与模型,描述了几种常见的安全模型:Lampson 模型、Graham-Denning 模型、Harrison-Ruzzo-Ullman 模型、Bell-LaPadula 模型、D. Denning 信息流模型、Biba 模型、Clark-Wilson 模型、Chinese-Wall 模型、RBAC 模型以及 Take-Grant 模型;第 7 章为安全操作系统的设计与实现,讲述了安全操作系统的设计原理、设计方法以及关键技术的实现;第 8 章为国内外安全操作系统介绍,讲述了国外三种著名的安全操作系统:SE-Linux、EROS 以及 DG UX/B2;第 9 章为安全操作系统评估,简要回顾了计算机信息系统的测评标准的发展历程,并详

细介绍了我国强制性国家标准《计算机信息系统安全保护等级划分准则》和国际通用标准《信息技术安全性评估通用准则(CC)》;第10章为安全操作系统的应用场景,描述了安全操作系统的几个重要的应用场景。

在本书的写作过程中,得到以下老师及同仁的大力帮助,在此对他们表示感谢。他们是:中国科学院信息安全国家重点实验室林东岱研究员,国家信息安全产品测评认证中心徐长醒博士,北京市信息安全测评中心刘海峰博士;中国科学院软件研究所季庆光博士、唐柳英博士、朱继锋博士、沈建军硕士、何昀峰硕士、郭丽和孙红艳硕士,等等。

由于作者水平、时间有限,书中错误在所难免,敬请各位读者批评并盼指正!

作 者

2004年2月于北京

目 录

第 1 章 绪论	1
1.1 计算机安全事件	1
1.2 数字威胁	3
1.2.1 安全威胁的根源	3
1.2.2 软件脆弱性报告	4
1.3 计算机安全	8
1.4 操作系统安全性的意义	9
1.4.1 操作系统的基础安全特性	10
1.4.2 操作系统安全性的基础作用	13
1.5 相关术语.....	15
思考题	16
第 2 章 通用操作系统的安全机制	17
2.1 Windows 操作系统安全机制	17
2.1.1 Windows NT/2000/XP 系统结构	17
2.1.2 Windows NT/2000/XP 安全模型	19
2.1.3 Windows NT/2000/XP 系统登录过程	24
2.1.4 Windows NT/2000/XP 资源访问	26
2.1.5 Windows NT/2000/XP 安全审计	35
2.2 Linux 操作系统的安全机制	36
2.2.1 身份标识与鉴别	37
2.2.2 自主访问控制	39
2.2.3 特权管理	39
2.2.4 安全审计	40
2.2.5 安全注意键	41
2.2.6 其他安全机制	42
思考题	49
第 3 章 安全操作系统研究的发展	50
3.1 引言	50
3.2 发展阶段划分方法	50
3.3 奠基时期	51

3.3.1 萌芽与访问控制抽象	51
3.3.2 引用监控器和安全核	52
3.3.3 隐蔽信道与 BLP 模型	54
3.3.4 保护机制结构与设计原则	55
3.3.5 操作系统保护理论	56
3.3.6 系统设计和开发	58
3.4 食谱时期	60
3.4.1 第一个计算机安全评价标准	60
3.4.2 LINUS IV 系统的开发	61
3.4.3 安全 XENIX 系统的开发	62
3.4.4 System V/MLS 系统的开发	64
3.4.5 安全 TUNIS 系统的开发	65
3.4.6 ASOS 系统的开发	66
3.5 多策略时期	67
3.5.1 国防部目标安全体系结构	67
3.5.2 多策略环境中的安全策略支持范型	68
3.5.3 基于 Mach 的 DTOS 安全操作系统	70
3.6 动态策略时期	72
3.6.1 基于 Fluke 的 Flask 安全操作系统	73
3.6.2 基于 Linux 的 SE-Linux 安全操作系统	75
3.7 中国的安全操作系统研究开发工作	76
思考题	78
第 4 章 安全需求与安全策略	79
4.1 安全需求	79
4.1.1 信息的机密性需求	80
4.1.2 信息的完整性需求	80
4.1.3 信息的可记帐性需求	81
4.1.4 信息的可用性需求	81
4.2 安全策略	81
4.2.1 定义	82
4.2.2 策略语言	83
4.2.3 安全策略的分类	88
4.3 访问控制策略	90
4.3.1 访问控制属性	91
4.3.2 自主访问控制策略	93

4.3.3 强制访问控制策略	94
4.4 访问支持策略	97
4.4.1 标识与鉴别	98
4.4.2 可记帐性	100
4.4.3 确切保证	101
4.4.4 连续保护	102
4.4.5 客体重用	102
4.4.6 隐蔽信道	103
4.5 DTE 策略	104
4.5.1 域的划分	105
4.5.2 型的划分	109
4.5.3 赋型规则	111
思考题	113
第5章 操作系统安全体系结构	114
5.1 安全体系结构的含义及类型	114
5.2 计算机系统的安全体系结构设计的基本原则	116
5.3 Flask 体系	119
5.3.1 背景介绍	119
5.3.2 策略灵活性分析	120
5.3.3 Flask 体系的设计与实现	122
5.3.4 特殊微内核特征	127
5.3.5 支持吊销机制	128
5.3.6 安全服务器	130
5.3.7 其他 Flask 对象管理器	131
5.3.8 LSM 访问控制框架	135
5.3.9 Flask 和 LSM 的结合	136
5.4 权能体系	137
5.4.1 权能的一般概念	138
5.4.2 对权能的控制及实现方法	138
5.4.3 权能系统的局限性	138
思考题	139
第6章 形式化方法与安全模型	140
6.1 形式化方法	140
6.2 形式化安全模型	144

6.3 基于访问控制矩阵的安全模型	146
6.3.1 Lampson 访问控制矩阵模型	146
6.3.2 Graham-Denning 模型	147
6.3.3 Harrison-Ruzzo-Ullman 模型	149
6.4 基于格的安全模型	151
6.4.1 Bell-LaPadula 模型介绍	151
6.4.2 D. Denning 信息流模型	159
6.4.3 Biba 模型	164
6.5 其他安全模型	168
6.5.1 Clark-Wilson 模型	168
6.5.2 Chinese-Wall 模型	170
6.5.3 RBAC 模型	177
思考题	184
第7章 安全操作系统的设计与实现	185
7.1 安全操作系统的设计原理	185
7.2 安全操作系统的设计	187
7.2.1 隔离	187
7.2.2 安全内核	191
7.2.3 分层设计	194
7.2.4 环结构	195
7.3 安全操作系统的开发	199
7.3.1 安全操作系统开发方法	199
7.3.2 安全操作系统开发过程	201
7.3.3 安全操作系统的开发	204
7.4 安全操作系统关键技术的实现	210
7.4.1 自主访问控制的实现	210
7.4.2 强制访问控制的实现	216
7.4.3 最小特权的实现	220
7.4.4 安全审计的实现	228
7.4.5 隐蔽信道分析	233
思考题	237
第8章 国外知名安全操作系统介绍	238
8.1 SE-LINUX 介绍	238
8.1.1 SE-Linux 体系结构简介	238

8.1.2 SE-Linux 中安全性标签的实现	240
8.1.3 SE-Linux 中的访问权限检查	241
8.1.4 SE-Linux 系统中的各子系统安全机制	243
8.2 EROS 介绍	249
8.2.1 EROS 的体系结构	250
8.2.2 能力与强制访问控制	255
8.2.3 EROS 内核	257
8.2.4 EROS 实现	262
8.2.5 EROS 系统服务	268
8.3 DG/UX B2 介绍	271
8.3.1 DG/UX B2 的安全体系结构	271
8.3.2 DG/UX B2 的安全特征	275
思考题	287
第9章 信息系统安全评估标准介绍	289
9.1 评估标准发展的趋势	289
9.2 评估标准的历史回顾	290
9.2.1 信息安全标准简介	290
9.2.2 不同标准的评估情况	298
9.2.3 实施评估的国家分布	299
9.3 计算机信息系统安全保护等级划分准则	299
9.3.1 第一级 用户自主保护级	299
9.3.2 第二级 系统审计保护级	300
9.3.3 第三级 安全标记保护级	301
9.3.4 第四级 结构化保护级	302
9.3.5 第五级 访问验证保护级	304
9.4 信息技术安全性评估通用准则(CC)	307
9.4.1 CC 结构	307
9.4.2 CC 的适用范围	308
9.4.3 CC 的目标读者	309
9.4.4 CC 的文档组织	309
9.4.5 CC 中的关键概念描述	310
9.4.6 CC 的安全功能类	311
9.4.7 CC 的安全保证类	321
9.4.8 CC 的安全保证级别	327
思考题	329

第 10 章 安全操作系统应用场景	330
10.1 安全操作系统应用	330
10.2 安全操作系统应用场景之一:对堆栈溢出攻击的防范	333
10.2.1 什么是堆栈溢出攻击	333
10.2.2 堆栈溢出攻击的原理	334
10.3 安全操作系统应用场景之二:对口令攻击的防范	346
10.3.1 口令攻击的原理	347
10.3.2 口令攻击的方法	348
10.3.3 安全操作系统对口令攻击的防范	349
10.4 安全操作系统应用场景之三:对计算机病毒的防范	351
10.4.1 计算机病毒的定义	351
10.4.2 计算机病毒的历史	352
10.4.3 计算机病毒的分类	353
10.4.4 计算机反病毒技术	359
10.4.5 安全操作系统对计算机病毒的防范	361
10.5 安全操作系统应用场景之四:对拒绝服务攻击的防范	363
10.5.1 拒绝服务攻击的定义	363
10.5.2 拒绝服务攻击的分类	365
10.5.3 从 DoS 到 DDoS	368
10.5.4 安全操作系统对拒绝服务攻击的防范	370
思考题	373
主要参考文献	374

第 1 章 绪 论

本章从发生在当前快速发展的信息化网络环境下的计算机安全事件讲起,描述这些计算机安全事件发生的本源,我们在数字世界中面临的威胁,进而引申出作为计算机系统的核心部件——安全操作系统的重要性。

1.1 计算机安全事件

随着计算机和互联网技术迅猛的发展,应用领域正在不断拓展,电子商务、公用网站、金融电子化等新兴事物的出现,极大地改变了人们传统的生活和学习方式。计算机技术的普及使得越来越多的人开始使用计算机,但是随着社会网络化程度的增加,开放式网络体系的安全性隐患日益明显地暴露出来。

1988 年的莫里斯蠕虫事件揭开了大规模网络攻击的序幕。虽然该程序的攻击方法很简单,但是它所造成的损失至今也难以清楚地估计。从此,网上不甘寂寞的好事者们纷纷效仿,制造了一系列骇人听闻的“黑客事件”。以下记录了来自各种消息源的计算机安全事件的新闻摘要:

1995 年 2 月,被认为世界上的头号黑客——凯文·米特尼克(Kevin Mitnick)终于再次被送上了法庭。美国联邦调查局从 1992 年就开始搜捕他,但直到 1995 年才在北卡罗来纳州的罗利将其抓获。因其在摩托罗拉、诺基亚、北电、太阳微系统等知名公司和南加州大学的网站上窃取软件并篡改数据,造成了数千万美元的损失而被判监禁 5 年。

1996 年初,法国国防部证实,法国海军参谋部计算机储备的军事机密于 1995 年 7 月被人窃走,其中包括几百艘盟军军舰的声音识别密码以及舰只航行图。

1997 年 11 月,中国工商银行青岛分行信用卡部一名工作人员利用工作之便解析信用卡密钥生成技术,制造假牡丹卡诈骗 70 多万元。在我国仅 1997、1998 两年,四家国有商业银行就发生计算机犯罪案件共 140 余起,涉及人员 160 多人,涉案金额 1.6 亿多元,造成很大经济损失。

1999 年 4 月 26 日,全世界至少有 6000 万台计算机遭受了 CIH 病毒的侵害,计算机系统瘫痪或硬盘分区表被改写,甚至许多机器的数据不可逆转地永久丢失掉了。这以后每到 4 月 26 日,甚至每月的 26 日,计算机用户们都心有余悸。梅莉莎病毒、蠕虫病毒、“我爱你”病毒等成为每年计算机安全事件的热门。

2000 年 2 月,以“雅虎”为首的美国一系列大型网站遭到了黑客有组织的攻

击。他们攻击的目标包括雅虎、电子港湾、亚马逊、微软网络等美国大型国际互联网网站。据统计,在 2 月 7~9 日这短短的三天里,这些受害公司的损失就超过了 10 亿美元,其中仅营销和广告收入一项便高达 1 亿美元。4 月份,在威尔斯少年黑客葛雷窃取的信用卡资料中,发现他顺便还看了微软总裁盖茨的资料,10 月中旬,微软的高度机密网络被一名来自俄罗斯的黑客入侵,在几周时间里,黑客攻破了微软的系统,并偷走了微软的部分源代码,从而引起全球恐慌。

2001 年 1 月,首都在线 263 的一个服务器受到黑客的攻击。该网站的页面被修改,而且黑客在网页上还“签上”了自己的名字。4 月 4 日,美国一些黑客组织相继对我国的一些政府、企业、教育、科研、电信等网站进行攻击。特别是中美撞机事件发生以来,我国的一些黑客组织忍无可忍,发起了一场网络反击战。这样,便引发了 IT 发展史上一个十分具有历史意义的事件——中美黑客大战。

2002 年 3 月某人闯入了 SalesGate.com 的 B2B(business-to-business)网站,窃取了约 3000 客户的记录,其中包括信用卡号以及其他个人信息。此人还在互联网上张贴了其中一些人的资料。

据联邦调查局统计,美国每年因网络安全造成的损失高达 75 亿美元。

据美国《金融时报》报道,世界上平均每 20 秒就发生一次入侵国际互联网的计算机安全事件,三分之一的防火墙被突破。

美国联邦调查局计算机犯罪组负责人吉姆·塞特尔称,给我精选 10 名黑客组成一个小组,90 天内,我将使美国趴下。

美国国防部对其军用计算机网络进行安全检测后所提出的报告中指出:现用网络中,85%的计算机可能受到侵害;15%曾有报警记录;5%曾有遭受过攻击的报告。

美国已生产出第一代采用“病毒固化”技术的芯片,并开始嵌入出口的计算机产品中。一旦需要,便可遥控激活。在海湾战争中,美国特工人员在安曼将伊拉克从德国进口的一批计算机打印设备中换上含有“可控计算机病毒”的芯片,导致伊方的计算机系统战争初期就陷入全面瘫痪。

据总部设在卡内基·梅隆大学软件工程学院的美国计算机紧急事件反应小组(CERT)的统计,1988 年发生的计算机安全事件仅 6 起,其中包括被认为是大规模互联网攻击的开端的“莫里斯蠕虫事件”,而到 2002 年底,计算机安全事件达到 82 094 起,而在 2003 年第 1 季度,计算机安全事件就达 42 586 起,自 1988 年统计以来到 2003 年第 3 季度,共计发生 297 318 起计算机安全事件。表 1.1 为自 1988 年以来,由 CERT 小组统计发生的计算机安全事件。

表 1.1 计算机安全事件

1988~1989

年份	1988	1989
事件	6	132

1990~1999

年份	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
事件	252	406	773	1 334	2 340	2 412	2 573	2 134	3 734	9859

2000~2003

年份	2000	2001	2002	1Q-3Q2003
事件	21 756	52 658	82 094	114 855

据初步统计,黑客事件仅在美国每年造成的经济损失就超过 100 亿美元。涉及政府机构、军事部门、科研院校、金融商业等部门的计算机犯罪,严重干扰了人们的日常生活,恶意侵犯公民隐私,造成巨大的经济损失,甚至直接或间接地威胁到国家安全。严峻的现实让人们清醒地意识到,计算机和网络的发展离不开信息安全技术的保障。随着人们安全意识的提高,安全领域的探索和研究正日益深入。世界各国都投入了大量的人力、物力和财力,不遗余力地提高计算机信息系统的安全性。

1.2 数字威胁

从计算机的发展历史来看,早期的计算机使用者集中在大学校园、研究团体这样的学术领域。在这种学术研究气氛浓郁的应用环境中,安全自然不是考虑的首要问题,功能全面和使用便捷才是人们所最关心的。这一观念沿袭至今,因而才有了大量使用简洁、行为古怪却又功能异常强大的 Unix 命令,诸如 cp, sed, grep, awk 等系统命令,缓冲区溢出的罪魁祸首 gets(), strcpy() 等系统库函数,以及 rservices, sendmail, finger, telnet, nis 等曾经引发一系列安全隐患的服务程序。长期以来,桌面 PC 机几乎毫无安全性可言,Unix 安全性也像“海市蜃楼”一样可望而不可及。

1.2.1 安全威胁的根源

原先彼此信任的前提条件在飞速发展的 Internet 计算环境中已经不再成立,