

计算机系统安全技术

李海泉 李 健 编著

人民邮电出版社

图书在版编目(CIP)数据

计算机系统安全技术/李海泉,李健编著.—北京:人民邮电出版社,2001.9

ISBN 7-115-09570-1

. 计 李 ... 李 电子计算机—安全技术 . TP309

中国版本图书馆 CIP 数据核字(2001)第 051561 号

内容提要

本书主要介绍计算机系统的安全技术及其方法。全书共 14 章,内容包括计算机系统的环境安全、实体安全、计算机的防电磁泄漏、软件安全技术、软件加密技术、操作系统的安全,数据库的安全与加密、网络安全与加密、局域网安全、计算机病毒的诊断与消除、系统的运行安全、计算机系统的安全管理、计算机系统的安全评估等。

本书内容全面,深入浅出,简明实用,可用作计算机科学技术及应用、软件工程及应用、信息工程、信息管理与信息系统、银行信息管理、会计信息管理和计算机安全等专业的工具书,也可以作为大专院校相关专业的教材,还可供相关专业的研究生学习和参考。

计算机系统安全技术

编 著 李海泉 李健

责任编辑 马 嘉

人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@pptph.com.cn

网址 <http://www.pptph.com.cn>

北京汉魂图文设计有限公司制作

北京 印刷厂印刷

新华书店总店北京发行所经销

开本:787×1092 1/16

印张:30

字数:721千字

2001年9月第1版

印数:1-000册

2001年9月北京第1次印刷

ISBN 7-115-09570-1/TP·2415

定价:44.00元

序 言

随着计算机科学技术的迅速发展和广泛应用,计算机系统的安全问题已成为人们十分关注的重要课题。计算机系统面临着两类严重的威胁和攻击。一类是对计算机实体的威胁和攻击,如各种自然灾害、场地和环境因素的影响、战争破坏和损失、人为破坏、设备故障、各种媒体设备的破坏和丢失。这不仅造成国家财产的严重损失,而且也会造成信息的泄漏和破坏。另一类是对信息的威胁和攻击,包括信息泄漏和信息破坏。信息泄漏即故意或偶然地侦收、截获、窃取、分析和收到系统中的信息,特别是机密和敏感信息,造成泄密事件。信息破坏是指由于偶然事故或人为因素破坏信息的完整性、正确性和可用性,尤其是计算机犯罪和计算机病毒,将导致信息被修改、删除和破坏,系统资源被盗或被非法使用,甚至使系统瘫痪。为了保证计算机系统的安全,计算机科学技术及应用、信息工程、软件工程、信息管理与信息系统、金融信息管理、会计信息管理等的专业科技人员和计算机安全人员,以及大专院校相关专业的师生,必须系统地学习和研究计算机系统安全技术与方法。

李海泉教授任中国计算机学会维护与管理专业委员会副主任、中国计算机学会外部设备专业委员会委员、中国计算机学会名词审定与编辑出版委员会委员、中国电子学会计算机工程与应用分会维护专业委员会副主任等职。他先后完成了多个国防科技和国家八五国防预研项目,获得了多项部级科技进步奖;发表过160多篇学术论文,编著并出版了15本专著、8种大专院校教材,获得5部“优秀科技著作奖”、“优秀教材奖”。1997年3月所出版的《计算机系统的安全技术与方法》一书经多年教学使用,读者反映良好,先后获得省教委“优秀教材奖”和本学会“优秀科技著作二等奖”。今年,李教授根据多年教学和科研实践经验,在原著作基础上,又参考了国内外有关学术著作,编写了《计算机系统安全技术》一书。本书具有以下特点:

1. 所介绍的理论方法具有先进性和通用性。例如,防电磁泄漏、抗电磁干扰、计算机安全保护、软件加密、数据加密、病毒的诊断和消除、网络安全保护、安全运行与管理等技术和方法,不会因计算机的更新换代而失去应用价值。

2. 实用性强,内容广泛,深入浅出。所介绍的理论与方法都很实用,并提供可参考和借鉴的程序或工具,可操作性很强,便于读者掌握。所选实例典型,可直接应用,并举一反三、触类旁通。

3. 编写方式独具风格。每章开头有内容提要,引导读者学习原理和方法。每章末有内容小结和习题与思考题,帮助读者复习、巩固所学知识。本书最后附有参考文献,可供读者深入研究,掌握所学的技术和方法。

本书可用作计算机科学及应用、信息工程、软件工程、信息管理与信息系统、银行信息管理、会计信息管理和计算机安全等专业的工具性参考书,也可以作为大专院校相应专业教材,还可供研究生学习和参考。

中国计算机学会计算机维护与管理专业委员会
编辑出版委员会
2000年9月

前 言

当今社会是科学技术高度发展的信息社会,人类的一切活动均离不开信息。随着社会的不断发展,各种各样的信息技术不断涌现。信息系统是以计算机及外部设备为基础,进行信息的收集、传输、存储、加工处理、分发和利用的系统,它的大量应用给人类创造了巨大的财富,同时也成为威胁、攻击和破坏的目标和对象。

对计算机系统的威胁和攻击主要有两类:一类是对计算机系统实体的威胁和攻击;一类是对信息的威胁和攻击。计算机犯罪和计算机病毒则包含了对实体和信息两个方面的威胁和攻击。计算机系统实体所面临的威胁和攻击主要指各种自然灾害、场地和环境因素的影响、战争破坏和损失、设备故障、人为破坏、各种媒体设备的损坏和丢失。对实体的威胁和攻击,不仅造成国家财产的严重损失,而且会造成信息的泄漏和破坏。因此,对计算机系统实体的安全保护是防止对信息威胁和攻击的有力措施。对信息的威胁和攻击主要有两种方式:一种是信息泄漏,一种是信息破坏。信息泄漏是指故意或偶然地侦收、截获、窃取、分析、收集到系统中的信息,特别是机密信息和敏感信息,造成泄密事件。信息的破坏是指由于偶然事故或人为因素破坏信息的完整性、正确性和可用性,如各种软硬件的偶然故障,环境和自然因素的影响以及操作失误造成的信息破坏,尤其是计算机犯罪和计算机病毒造成信息的修改、删除或破坏,将导致系统资源被盗或被非法使用,甚至使系统瘫痪。为了保证计算机系统的安全性,必须系统、深入地研究计算机系统的安全技术与方法。

目前,国内尚缺乏全面、系统地介绍计算机安全技术与方法方面的专著和教材。现有的书或者从某个侧面介绍计算机的安全技术,或者是纯理论的阐述,缺乏实用价值。本书作者曾编著了《计算机系统安全技术与方法》教材,经多年教学与科研实践,又参考了大量国内外文献资料,在此基础上,编写了本书,旨在使计算机应用、信息系统开发、使用、维护和管理的技术人员和大专院校计算机科学技术及应用、软件工程及应用、信息工程、信息管理与信息系统、会计信息管理,金融信息管理和计算机安全管理等专业的师生重视计算机系统的安全问题,更多地了解和掌握这门学科的基本原理、方法、技术和工具,了解本学科研究的范围和内容,使自己的计算机系统和信息系统更加安全、可靠,更加实用。

本书共包括 14 章和 3 个附录,比较全面、系统地介绍了计算机系统安全概论、环境安全、实体安全、抗电磁干扰、防电磁泄漏、软件安全技术、软件加密技术、操作系统的安全、数据库的安全与加密、网络安全与数据加密、局域网安全、计算机病毒的诊断与消除、系统运行安全、系统的安全管理、计算机系统的安全评估,以及计算机信息的安全保护条例、计算机网络国际联网管理办法,美国计算机系统安全评估准则三个附录。本书内容广泛,深入浅出,简明实用,理论性和实用价值高,可操作性很强。每章有小结和习题与思考题,书后附有参考文献,可供复习和深入研究。

本书在编写时,国家教委高校计算机教学指导委员会委员、国家高校计算机软件教材编审委员会委员、中国微机学会理事、西北大学计算机科学系郝克刚教授,仔细审阅了编写大纲和部分手稿,西安电子科技大学计算机系陈家正教授、西北大学计算机科学系卞雷教授、西安邮电学院孙公达教授仔细审阅过本书手稿,提出了宝贵意见。本书在编写中,还得到了我

院、系有关领导和老师们的关心和支持。我院学生张莉、万芳、王馨、吕凯元、孙雅水、程德玉、朱艳等帮助抄写了有关手稿,青年教师李刚、李健帮助进行了部分录入工作。在此,一并表示衷心的感谢。

由于作者水平有限,书中疏漏之处在所难免,敬请广大读者批评指正。

作 者

目 录

第一章 绪论	1
1.1 计算机系统面临的威胁和攻击	1
1.1.1 对实体的威胁和攻击	1
1.1.2 对信息的威胁和攻击	2
1.1.3 计算机犯罪	4
1.1.4 计算机病毒	7
1.2 计算机系统的脆弱性	8
1.2.1 系统的脆弱性	8
1.2.2 影响系统安全的因素	10
1.3 计算机系统安全的重要性	11
1.3.1 系统安全的重要性	11
1.3.2 计算机的安全要求	12
1.4 计算机系统的安全对策	13
1.4.1 安全对策的一般原则	13
1.4.2 安全策略的职能	14
1.4.3 安全机制	14
1.4.4 安全对策与安全措施	16
1.5 计算机系统的安全技术	17
1.5.1 计算机系统的安全需求	17
1.5.2 安全系统的设计原则	18
1.5.3 计算机系统的安全技术	19
1.5.4 可信计算机	21
1.5.5 容错计算机	22
本章小结	22
习题与思考题	23
第二章 计算机系统的环境安全	24
2.1 计算机系统安全的环境条件	24
2.1.1 温度	24
2.1.2 湿度	25
2.1.3 洁净度	26
2.1.4 腐蚀和虫害	27
2.1.5 振动和冲击	28
2.1.6 噪音及电气干扰	28
2.2 计算机房的安全等级	30

2.3	机房场地环境选择	31
2.3.1	外部环境	32
2.3.2	内部环境	33
2.4	机房的建造	33
2.4.1	机房的组成	33
2.4.2	各类房间的布局	34
2.4.3	机房面积的计算	34
2.4.4	机房的建筑结构	35
2.4.5	机房设备的布局	35
2.5	机房的装修	36
2.5.1	地板	36
2.5.2	吊顶	36
2.5.3	墙面	36
2.5.4	门窗	37
2.5.5	隔断	37
2.5.6	机房照明	37
2.5.7	机房的色彩	38
2.6	计算机的安全防护	38
2.6.1	防火	38
2.6.2	防水	40
2.6.3	防震	41
2.6.4	安全供电	41
2.6.5	防盗	41
2.6.6	防物理、化学和生物灾害	42
	本章小结	42
	习题与思考题	43
第三章	计算机系统实体的安全	44
3.1	计算机系统的可靠性	44
3.1.1	计算机系统的可靠性	44
3.1.2	计算机系统的故障分析	45
3.1.3	计算机系统故障的原因	46
3.2	计算机的故障诊断	47
3.2.1	人工诊断	47
3.2.2	功能测试法	49
3.2.3	微程序诊断	50
3.2.4	几种故障诊断方法比较	51
3.3	计算机的抗电磁干扰	51
3.3.1	来自计算机内部的电磁干扰	52

3.3.2	来自计算机外部的电磁干扰	53
3.3.3	计算机中电磁干扰的耦合形式	55
3.3.4	计算机中的干扰抑制技术	56
3.3.5	我国的电磁兼容性标准	59
3.4	实体的访问控制	59
3.4.1	访问控制的基本任务	60
3.4.2	实体访问控制	61
3.4.3	身份的鉴别	61
3.5	记录媒体的保护与管理	65
3.5.1	记录媒体的分类	65
3.5.2	记录媒体的防护要求	66
3.5.3	记录媒体的使用与管理状况	66
3.5.4	磁记录媒体的管理	67
	本章小结	69
	习题与思考题	69
第四章	计算机的防电磁泄漏	71
4.1	计算机的电磁泄漏特性	71
4.1.1	辐射场特性	72
4.1.2	传导场特性	73
4.1.3	影响电磁辐射强度的因素	75
4.2	对计算机辐射信息的接收与测试	75
4.2.1	对计算机辐射信息的接收与恢复	75
4.2.2	计算机泄漏电磁信息的测试仪器	75
4.2.3	对计算机设备辐射泄漏的测量	78
4.2.4	对计算机设备传导泄漏的测量	78
4.3	计算机的 TEMPEST 技术	79
4.3.1	TEMPEST 研究的内容	79
4.3.2	计算机中的 TEMPEST 技术	80
4.4	计算机的简易防泄漏措施	81
4.5	外部设备的 TEMPEST 技术	82
4.5.1	键盘的 TEMPEST 技术	82
4.5.2	软盘驱动器	83
4.5.3	显示终端	83
4.5.4	打印机	83
4.6	计算机设备的电磁辐射标准	83
4.7	发展我国的 TEMPEST 技术	87
	本章小结	89
	习题与思考题	90

第五章 计算机软件安全技术	91
5.1 软件安全的基本技术概述	91
5.1.1 防拷贝	91
5.1.2 防静态分析	95
5.1.3 防动态跟踪	98
5.2 软件防拷贝技术	100
5.2.1 激光孔加密技术	101
5.2.2 电磁加密技术	105
5.2.3 掩膜技术	106
5.3 磁道软标记加密法	106
5.3.1 磁道接缝加密法	106
5.3.2 宽磁道加密法	107
5.3.3 未格式化磁道加密法	108
5.3.4 螺线型磁道加密法	109
5.4 扇段软标记加密法	110
5.4.1 扇区间隙软指纹加密法	110
5.4.2 异常 ID 加密法	111
5.4.3 超级扇段加密法	112
5.4.4 磁道扇区乱序排列加密法	113
5.4.5 未格式化扇区加密法	114
5.4.6 扇段对齐加密法	115
5.5 其他软标记加密法	116
5.5.1 利用错误 CRC 码加密	116
5.5.2 磁道噪声法	116
5.5.3 双机加密法	117
5.5.4 卷标加密法	118
5.5.5 弱位加密法	118
5.5.6 ID ROM 加密法	118
5.5.7 利用加密器进行加密	119
5.5.8 利用 CMOS RAM 芯片对程序加密	119
5.5.9 利用 KEPROM 加密	121
5.6 文件目录与子目录的加密	121
5.6.1 文件目录的加密	121
5.6.2 子目录的加密	126
5.7 硬盘防拷贝技术	129
5.7.1 主引导扇区设置密码防拷贝	130
5.7.2 利用文件首簇号防拷贝	131
5.7.3 磁盘的消隐与还原	134

5.7.4 硬盘加密、解密实例	135
5.8 防动态跟踪技术	138
5.8.1 跟踪的工具及其实现	138
5.8.2 防动态跟踪的方法	140
本章小结	151
习题与思考题	152
第六章 密码学与软件加密	153
6.1 密码学与软件加密概述	153
6.2 换位加密法	154
6.2.1 以字节为单位的换位加密方法	155
6.2.2 以比特为单位的换位加密方法	157
6.3 代替密码加密法	161
6.3.1 单表代替法	161
6.3.2 多表代替法	162
6.3.3 加减法	165
6.3.4 异或运算法	166
6.4 综合加密与乘积加密	167
6.4.1 综合加密	167
6.4.2 乘积加密	170
6.5 软件加密工具及其应用	173
6.5.1 评价软件加密工具的标准	173
6.5.2 软件加密工具及其应用	175
6.6 可执行文件的加密	177
6.6.1 .COM 类文件的加密	177
6.6.2 .EXE 类文件的加密	178
6.6.3 .BAT 类文件的加密	180
6.7 BASIC 程序的加密	182
6.7.1 用 P 参数加密	182
6.7.2 P 参数加密文件的解密	184
6.7.3 BASIC 源程序关键字变码加密	184
6.7.4 BASIC 源程序的编译加密	188
6.8 口令加密与限制技术	188
6.8.1 口令加密技术	188
6.8.2 限制技术	192
6.9 加密算法的可靠性	194
本章小结	197
习题与思考题	198

第七章 操作系统的安全	199
7.1 操作系统的安全问题	199
7.2 操作系统的安全控制	200
7.2.1 操作系统的安全控制方法	200
7.2.2 访问控制的基本理论	201
7.2.3 访问控制的方式	202
7.2.4 访问控制的方法	202
7.2.5 用户身份的识别与验证	204
7.3 自主访问控制	206
7.3.1 自主访问控制方法	206
7.3.2 自主访问控制的访问类型	207
7.3.3 自主访问控制的访问模式	208
7.4 强制访问机制	209
7.5 存储器的保护	210
7.5.1 存储器的保护方法	210
7.5.2 存储器的管理	212
7.5.3 虚拟存储器的保护	214
7.6 操作系统的安全设计	214
7.6.1 操作系统的安全模型	214
7.6.2 安全操作系统的设计原则	216
7.6.3 安全操作系统的设计方法	217
7.6.4 对系统安全性的认证	217
7.7 I/O设备的访问控制.....	218
7.7.1 I/O设备访问控制.....	218
7.7.2 输入安全控制	219
7.8 几种操作系统的安全性	220
7.8.1 DOS系统的安全性	220
7.8.2 Windows和Windows NT的安全性	221
7.8.3 UNIX系统的安全性	222
本章小结.....	222
习题与思考题.....	224
第八章 数据库的安全与加密.....	225
8.1 数据库安全概述	225
8.1.1 数据库安全的重要性	225
8.1.2 数据库的安全问题	226
8.1.3 数据库面临的安全威胁	226
8.1.4 数据库的安全需求	227

8.2	数据库的安全策略与安全评价	229
8.2.1	数据库的安全策略	229
8.2.2	数据库的审计	230
8.2.3	数据库的安全评价	231
8.3	安全模型与安全控制	232
8.3.1	数据库的安全模型	232
8.3.2	数据库的安全控制	234
8.3.3	数据库的安全检查	235
8.4	数据库的安全技术	236
8.4.1	口令保护	236
8.4.2	数据加密	237
8.4.3	数据库加密	237
8.4.4	数据验证	238
8.5	数据库的加密	239
8.5.1	数据库的加密要求	239
8.5.2	数据库的加密方式	239
8.5.3	数据库文件的加密	240
8.6	数据库文件的保护	246
8.7	数据库命令文件的加密	250
8.7.1	数据库保密口令的设置	250
8.7.2	数据库命令文件的加密	253
8.7.3	数据库命令文件的编译	254
8.8	数据库的保密程序及其应用	254
8.8.1	Protect 的保密功能	254
8.8.2	Protect 功能的应用	255
8.9	Oracle 数据库的安全	256
8.9.1	Oracle 的访问控制	257
8.9.2	Oracle 的完整性	258
8.9.3	Oracle 的并发控制	258
8.9.4	Oracle 的审计追踪	261
	本章小结	262
	习题与思考题	263
第九章 网络安全与数据加密		264
9.1	OSI 网络安全体系结构	264
9.2	网络安全面临的威胁	266
9.2.1	网络部件的不安全因素	266
9.2.2	软件的不安全因素	267
9.2.3	工作人员的不安全因素	268

9.2.4	环境的不安全因素	269
9.3	网络安全策略和安全机制	269
9.3.1	网络安全策略	269
9.3.2	网络安全机制	270
9.4	网络安全对策与技术和网络的安全功能	270
9.4.1	网络的安全对策与技术	270
9.4.2	网络的安全目标	272
9.4.3	网络的安全功能	273
9.4.5	安全功能在 OSI 结构中的位置	274
9.5	网络的访问控制和路由选择	275
9.5.1	网络的访问控制	275
9.5.2	路由选择控制	277
9.6	信息流分析控制与网络数据加密技术	280
9.6.1	信息流分析控制	280
9.6.2	网络数据加密技术	281
9.7	DES 数据加密	283
9.7.1	DES 加密算法	284
9.7.2	DES 加密的实现	291
9.7.3	对 DES 加密的评价与改进	296
9.8	IDEA 和 RSA 数据加密	298
9.8.1	IDEA 数据加密	298
9.8.2	RSA 数据加密	300
9.9	报文鉴别与数字签名	302
9.9.1	鉴别技术	302
9.9.2	数字签名	305
9.10	密钥的管理	308
9.10.1	密钥的管理问题	308
9.10.2	密钥的种类和作用	309
9.10.3	密钥的生成	310
9.10.4	密钥的保护	311
	本章小结	314
	习题与思考题	316
第十章	局域网的安全	317
10.1	局域网的可靠性	317
10.2	局域网的安全技术	317
10.3	网络访问控制	319
10.4	网络的分层构造	320
10.5	通信线路的安全保护	320

10.5.1	通信线路的安全问题	320
10.5.2	通信线路的安全保护	321
10.5.3	电话机的安全保护	322
10.6	传输安全控制	323
10.7	网络终端和工作站的安全	325
10.7.1	网络工作站和终端的访问控制	325
10.7.2	终端和工作站的审计追踪	325
10.7.3	闯入活动的检查方法	326
10.8	Novell 网的安全措施	327
10.8.1	入网保护	327
10.8.2	代管权保护	327
10.8.3	继承权保护	328
10.8.4	文件与目录属性的保护	328
	本章小结	328
	习题与思考题	330
第十一章	计算机病毒的诊断与消除	331
11.1	计算机病毒概述	331
11.1.1	计算机病毒的概念及特性	331
11.1.2	计算机病毒的起源与种类	332
11.2	计算机病毒的结构和破坏机理	336
11.2.1	计算机病毒的结构	336
11.2.2	计算机病毒的流程和破坏机理	338
11.3	计算机病毒的传播	339
11.3.1	病毒的传播过程	339
11.3.2	对几种计算机病毒的剖析	343
11.4	对宏病毒的分析	348
11.4.1	一般宏病毒	348
11.4.2	电子邮件宏病毒	350
11.5	计算机病毒的防范	351
11.5.1	计算机病毒的防范机理	351
11.5.2	计算机病毒的预防措施	351
11.5.3	计算机病毒预防软件	354
11.5.4	利用 Norton 工具进行磁盘信息修复	357
11.6	计算机病毒的特征	360
11.7	计算机病毒的检测与消除	364
11.7.1	病毒的检测方法	364
11.7.2	病毒的实用检查方法	365
11.7.3	病毒的检测工具	369

11.7.4	病毒检测软件及其应用	373
11.7.5	病毒消除软件及其应用	374
11.7.6	宏病毒的防治	379
11.7.7	手工清除计算机病毒	380
11.8	病毒与防病毒技术的新进展	382
11.8.1	早期病毒及其防治	382
11.8.2	隐型病毒及其防治	382
11.8.3	多态型病毒及其防治	383
11.8.4	计算机病毒的新发展	384
11.8.5	KV300 的功能及其应用	386
11.9	目前常见的计算机病毒	388
11.9.1	攻击 BOOT 扇区和主引导扇区的病毒	388
11.9.2	攻击文件的病毒	389
11.9.3	攻击计算机网络的病毒	392
11.9.4	73 种常见病毒特征	393
	本章小结	396
	习题与思考题	397
第十二章 系统的运行安全		399
12.1	系统的安全运行与管理	399
12.1.1	安全目标与安全管理	399
12.1.2	建立科学的机房管理制度	401
12.1.3	帮助用户用好计算机	402
12.2	计算机系统的维护	403
12.3	机房环境的监测及维护	405
12.4	计算机的随机故障维修	407
12.5	软件的可靠性与可维性	409
12.5.1	软件的可靠性	409
12.5.2	软件错误的特征	410
12.5.3	软件的可维性	411
12.6	操作系统的故障分析及处理	411
12.6.1	系统安装故障	411
12.6.2	系统引导故障	412
12.6.3	系统读/写操作故障	414
12.6.4	病毒感染故障	414
12.7	Windows 系统的故障分析与处理	415
12.7.1	Windows 的安装故障	415
12.7.2	Windows 的启动故障	416
12.7.3	Windows 的运行故障	417

12.7.4 Windows 的关闭故障	418
本章小结	420
习题与思考题	421
第十三章 计算机的安全管理与执法	422
13.1 计算机安全管理的内容和任务	422
13.2 加强计算机用户的安全意识	422
13.3 建立计算机安全管理机构	423
13.4 完善和加强计算机的管理功能	424
13.4.1 完善计算机的管理功能	424
13.4.2 加强对用户账号和口令的管理	424
13.4.3 加强计算机系统及网络的安全管理	424
13.5 计算机的安全管理	425
13.5.1 与安全有关的活动	425
13.5.2 人员的管理	425
13.5.3 安全管理的原则	426
13.5.4 物理屏障和管理规则	427
13.6 加强计算机立法和执法力度	427
13.6.1 加强计算机安全的立法	427
13.6.2 加强计算机法执行力度	428
本章小结	428
习题与思考题	429
第十四章 计算机系统的安全评估	430
14.1 计算机系统安全评估的目的和重要性	430
14.2 制定计算机系统安全标准的策略	431
14.3 计算机系统的安全要求	432
14.4 系统安全标准的制定	433
14.5 系统的安全评价方法	435
14.6 计算机的安全等级	437
14.6.1 非保护级	437
14.6.2 自主保护级	437
14.6.3 强制安全保护级	438
14.6.4 验证安全保护级	440
14.7 信息技术安全评估准则	440
14.8 计算机网络安全等级	442
14.8.1 安全要求	442
14.8.2 安全服务	445
本章小结	446

习题与思考题	447
附录	448
附录一 中华人民共和国计算机信息系统安全保护条例	448
附录二 计算机信息网络国际联网安全保护管理办法	450
附录三 美国计算机系统安全评价标准	453
参考文献	458