



全国高校出版社优秀畅销书

高等学校计算机科学与技术教材

- ④ 原理与技术的完美结合
- ④ 教学与科研的最新成果
- ④ 语言精炼，实例丰富
- ④ 可操作性强，实用性突出

计算机网络安全教程

(修订本)

□ 石志国 薛为民 尹 浩 编著

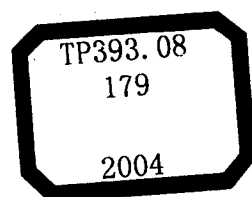
清华大学出版社



北京交通大学出版社



全国高校出版社优秀畅销书
高等学校计算机科学与技术教材



计算机网络安全教程

(修订本)

石志国 薛为民 尹 浩 编著

清华大学出版社
北京交通大学出版社

·北京·

内 容 简 介

本书是《计算机网络安全教程》的修订本,在原书基础上做了大量修整和扩充,使之更加适合高校教学和自学的需要。利用大量的实例讲解知识点,将安全理论、安全工具与安全编程三方面内容有机地结合到一起。每章最后都配有大量的习题,用来检查教学和学习进度。

全书从网络安全体系上分成四部分。第一部分:计算机网络安全基础,介绍网络安全的基本概念、实验环境配置、网络协议基础及网络安全编程基础。第二部分:网络安全攻击技术,详细介绍攻击技术“五部曲”及恶意代码的发展和原理。第三部分:网络安全防御技术,介绍安全操作系统相关原理、加密与解密技术的应用、防火墙、入侵检测技术及IP和Web安全相关理论。第四部分:网络安全综合解决方案,从工程的角度介绍网络安全工程方案的编写。

本书可以作为高校及各类培训机构相关课程的教材或者参考书。

本书中的源代码、所涉及的软件和授课幻灯片等教学支持信息可以从图书支持网站<http://www.gettop.net>下载,也可以从出版社网站<http://press.bjtu.edu.cn>的下载栏目中下载。

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

本书防伪标签采用特殊防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

计算机网络安全教程/石志国,薛为民,尹浩编著.一修订本.一北京:清华大学出版社;北京交通大学出版社,2007.1

(高等学校计算机科学与技术教材)

ISBN 978-7-81082-249-7

I. 计… II. ①石… ②薛… ③尹… III. 计算机网络-安全技术-高等学校-教材
IV. TP393.08

中国版本图书馆CIP数据核字(2006)第126904号

责任编辑:谭文芳

出版发行:清华大学出版社 邮编:100084 电话:010-62776969 <http://www.tup.com.cn>

北京交通大学出版社 邮编:100044 电话:010-51686414 <http://press.bjtu.edu.cn>

印刷者:北京东光印刷厂

经 销:全国新华书店

开 本:185×260 印张:21.5 字数:550千字

版 次:2004年2月第1版 2007年1月第1次修订 2007年2月第8次印刷

书 号:ISBN 978-7-81082-249-7/TP·101

印 数:35 001~45 000册 定价:31.00元

本书如有质量问题,请向北京交通大学出版社质监组反映。对您的意见和批评,我们表示欢迎和感谢。

投诉电话:010-51686043,51686008;传真:010-62225406;E-mail: press@center.bjtu.edu.cn。

修订本前言

修订本在原书基础上做了大量修整和扩充,使之更加适合高校教学和自学的需要。本书利用大量的实例讲解知识点,将安全理论、安全工具与安全编程三方面内容有机地结合到一起,每章最后都配有大量的习题,用来检查教学和学习的进度。

与第一版比较

2004年初《计算机网络安全教程》出版,目的是为了满足不同网络安全技术教学的迫切需要。该书综合了作者在北京大学计算机研究所部分研究内容、清华大学计算机系部分教学内容及网络信息安全国际认证考试的部分内容,在写作过程中还得到了三院院士王选老师的支持和指导。

原书出版以来,受到了老师、同学及广大读者的认可和欢迎,同时,很多读者也提出了很多改进意见。当前,网络安全是计算机相关领域中的一门重要学科,很多高校和研究机构都设置了网络信息安全本科专业及网络信息安全方向的硕士点和博士点。这次花了大量的时间对原书做了一次全面的更新,希望能更好的帮助广大读者学习好网络安全的相关知识。

修订本在保证原书整体结构的情况下,对内容进行了全面的扩充和修正,一个主要的特点是理论性的增强,主要做了如下6方面的调整。

(1) 增强了理论性并全面阐述了网络安全两个重要的概念:恶意代码和 Web 安全。添加了两章,分别为恶意代码分析与防治和 IP 安全与 Web 安全(修订本第 11 章),将全书扩充为 12 章。

(2) 修正并解决了部分内容不规范、图表不清楚的问题。

(3) 全面扩充了拒绝服务攻击及分布式拒绝服务攻击的分类和原理。

(4) 增加了安全操作系统的机制与原理。

(5) 增加了数字签名、数字水印和公钥基础设施 PKI 的相关内容。

(6) 为了检查教学及自学的效果,每章都重新设计了课后习题的内容,并给出了相关参考答案。

本书结构

修订本在每一章前面精心设计了“本章要点”,因为每一章内容都比较庞杂,所以要注意本章要点,重点掌握提及的内容。每一章后面都精心设计了适量的习题,主要是针对本章重点、难点进行训练。附录还提供了选择题和填空题的答案,可以对照检查自己的学习效果。对于简答题,均可以在书上找到答案。

本书导读

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性的科学。本书从计算机网络安全理论、网络安全攻防工具

和网络安全编程三个角度介绍计算机网络安全技术,这三方面内容均来自工程和课堂教学的实践,并通过网络安全攻防体系结合在一起。从网络安全攻防体系上,全书分成四部分,共12章。

第一部分:计算机网络安全基础

第1章 网络安全概述与环境配置。介绍信息安全和网络安全的研究体系、研究网络安全的意义、评价网络安全的标准及实验环境的配置。

第2章 网络安全协议基础。介绍 OSI 参考模型和 TCP/IP 协议族,实际分析 IP、TCP、UDP、ICMP 协议的结构及工作原理、网络服务和网络命令。

第3章 网络安全编程基础。介绍网络安全编程的基础知识、C 语言发展的四个阶段,以及网络安全编程的常用技术:Socket 编程、注册表编程及驻留编程,等等。

第二部分:网络安全的攻击技术

第4章 网络扫描与网络监听。介绍黑客及黑客攻击的基本概念,如何利用工具实现网络踩点、网络扫描和网络监听。

第5章 网络入侵。介绍常用的网络入侵技术:社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

第6章 网络后门与网络隐身。介绍网络后门和木马的基本概念,并利用四种方法实现网络后门;介绍利用工具实现网络跳板和网络隐身。

第7章 恶意代码分析与防治。介绍恶意代码的发展史,恶意代码长期存在的原因,介绍恶意代码实现机理、定义及攻击方法等。

第三部分:网络安全的防御技术

第8章 安全操作系统基础。介绍 UNIX、Linux 和 Windows 的特点,着重介绍安全操作系统的原理,介绍 Windows 操作系统的安全配置方案。

第9章 密码学与信息加密。介绍密码学的基本概念,DES 加密算法的概念及如何利用程序实现,RSA 加密算法的概念及实现算法,PGP 加密的原理和实现。

第10章 防火墙与入侵检测。介绍防火墙的基本概念、分类、实现模型,以及如何利用软件实现防火墙的规则集;介绍入侵检测系统的概念、原理,以及如何利用程序实现简单的入侵系统。

第11章 IP 安全与 Web 安全。介绍 IPSec 的必要性,IPSec 中的 AH 协议和 ESP 协议、密钥交换协议 IKE 和 VPN 的解决方案等。

第四部分:网络安全综合解决方案

第12章 网络安全方案设计。从网络安全工程的角度介绍网络安全方案编写的注意点及评价标准。

致谢

在编写过程中,得到众多老师的指导和帮助。感谢中科院软件所卿斯汉研究员、梁洪亮博士、商清华博士、周启明博士、张宏博士和金洁华工程师。感谢清华大学计算机系林闯主任。感谢北京科技大学王志良教授、徐正光教授、解仑副教授和王莉副教授。感谢中央广播电视大学崔林教授、徐孝凯教授、田萧老师和王春风老师。感谢中国软件行业协会邱钦伦高级工程师。感谢他们为本书提供了大量并且详尽的编程资料,并为本书解决了很多编程方面的问题。尤其要感谢的是北京交通大学出版社编辑谭文芳老师,她的支持是本书能顺利出版的关键。

感谢众多老师和同学们的支持,他们的每一个问题,都是本书要强调并解决的知识点,他们的认可是我最大的动力,本书献给你们,献给最广大的读者。

图书支持

本书可以作为高校及各类培训机构相关课程的教材或者教学参考书,网络安全自学人员和网络安全开发人员的参考书。本书提供完整的教学幻灯片、书中的所有软件和源代码及相关学习资源,将在 <http://www.gettop.net> 或者 <http://press.bjtu.edu.cn> 下载栏目中发布,欢迎访问和下载。

由于作者水平和时间有限,难免出现错误,对于本书的任何问题请使用E-mail发送到作者邮箱:shizhiguo@tom.com。

石志国
2007 年 1 月

目 录

第一部分 计算机网络安全基础

第 1 章 网络安全概述与环境配置	3
1.1 信息安全概述	3
1.1.1 信息安全研究层次	3
1.1.2 信息安全的基本要求	4
1.1.3 信息安全的发展	4
1.1.4 可信计算概述	5
1.2 网络安全概述	5
1.2.1 网络安全的攻防体系	5
1.2.2 网络安全的层次体系	6
1.3 研究网络安全的必要性	7
1.3.1 物理威胁	7
1.3.2 系统漏洞威胁	8
1.3.3 身份鉴别威胁	8
1.3.4 线缆连接威胁	9
1.3.5 有害程序威胁	9
1.4 研究网络安全的社会意义	9
1.4.1 网络安全与政治	9
1.4.2 网络安全与经济	10
1.4.3 网络安全与社会稳定	10
1.4.4 网络安全与军事	10
1.5 网络安全的相关法规	11
1.5.1 我国立法情况	11
1.5.2 国际立法情况	11
1.6 网络安全的评价标准	12
1.6.1 我国评价标准	12
1.6.2 国际评价标准	12
1.7 环境配置	14
1.7.1 安装 VMware 虚拟机	14
1.7.2 配置 VMware 虚拟机	16
1.7.3 网络抓包软件 Sniffer	22
1.7.4 使用 Sniffer 抓包	22
小结	26
课后习题	27
第 2 章 网络安全协议基础	28

2.1	OSI 参考模型	28
2.2	TCP/IP 协议族	30
2.2.1	TCP/IP 协议族模型	30
2.2.2	解剖 TCP/IP 模型	30
2.2.3	TCP/IP 协议族与 OSI 参考模型对应关系	31
2.3	网际协议 IP	31
2.3.1	IP 协议的头结构	31
2.3.2	IPv4 的 IP 地址分类	34
2.3.3	子网掩码	35
2.4	传输控制协议 TCP	36
2.4.1	TCP 协议的头结构	36
2.4.2	TCP 协议的工作原理	38
2.4.3	TCP 协议的“三次握手”	39
2.4.4	TCP 协议的“四次挥手”	40
2.5	用户数据报协议 UDP	42
2.5.1	UDP 协议和 TCP 协议的区别	42
2.5.2	UDP 协议的头结构	43
2.5.3	UDP 数据报分析	43
2.6	因特网控制消息协议 ICMP	45
2.6.1	ICMP 协议的头结构	45
2.6.2	ICMP 数据报分析	45
2.7	常用的网络服务	45
2.7.1	FTP 服务	46
2.7.2	Telnet 服务	47
2.7.3	E-mail 服务	49
2.7.4	Web 服务	49
2.7.5	常用的网络服务端口	49
2.8	常用的网络命令	49
2.8.1	ping 指令	50
2.8.2	ipconfig 指令	50
2.8.3	netstat 指令	51
2.8.4	net 指令	52
2.8.5	at 指令	54
2.8.6	tracert 指令	54
	小结	55
	课后习题	55
第 3 章	网络安全编程基础	57
3.1	网络安全编程概述	57
3.1.1	Windows 内部机制	57
3.1.2	学习 Windows 下的编程	59
3.1.3	选择编程工具	59
3.2	C 语言发展的 4 个阶段	63
3.2.1	面向过程的 C 语言	63

3.2.2 面向对象的 C++ 语言	65
3.2.3 SDK 编程	69
3.2.4 MFC 编程	75
3.3 网络安全编程	81
3.3.1 Socket 编程	81
3.3.2 注册表编程	83
3.3.3 文件系统编程	89
3.3.4 定时器编程	92
3.3.5 驻留程序编程	94
3.3.6 多线程编程	101
小结	104
课后习题	104

第二部分 网络安全的攻击技术

第 4 章 网络扫描与网络监听	109
4.1 黑客概述	109
4.1.1 黑客分类	109
4.1.2 黑客精神	110
4.1.3 黑客守则	110
4.1.4 攻击五部曲	110
4.1.5 攻击和安全的关系	111
4.2 网络踩点	111
4.3 网络扫描	111
4.3.1 网络扫描概述	112
4.3.2 被动式策略扫描	112
4.3.3 主动式策略扫描	119
4.4 网络监听	121
小结	124
课后习题	124
第 5 章 网络入侵	125
5.1 社会工程学攻击	125
5.2 物理攻击与防范	125
5.2.1 获取管理员密码	126
5.2.2 权限提升	127
5.3 暴力攻击	128
5.3.1 字典文件	128
5.3.2 暴力破解操作系统密码	129
5.3.3 暴力破解邮箱密码	129
5.3.4 暴力破解软件密码	130
5.4 Unicode 漏洞专题	132
5.4.1 Unicode 漏洞的检测方法	132
5.4.2 使用 Unicode 漏洞进行攻击	135

5.5 其他漏洞攻击	138
5.5.1 利用打印漏洞	138
5.5.2 SMB 致命攻击	139
5.6 缓冲区溢出攻击	140
5.6.1 RPC 漏洞溢出	141
5.6.2 利用 IIS 溢出进行攻击	142
5.6.3 利用 WebDav 远程溢出	145
5.7 拒绝服务攻击	149
5.7.1 SYN 风暴	150
5.7.2 Smurf 攻击	151
5.7.3 利用处理程序错误进行攻击	152
5.8 分布式拒绝服务攻击	153
5.8.1 DDoS 的特点	153
5.8.2 攻击手段	154
5.8.3 DDoS 的著名攻击工具	154
5.8.4 拒绝服务攻击的发展趋势	155
5.9 防范拒绝服务攻击	156
小结	157
课后习题	157
第 6 章 网络后门与网络隐身	159
6.1 网络后门	159
6.1.1 留后门的艺术	159
6.1.2 常见后门工具的使用	159
6.1.3 连接终端服务的软件	169
6.1.4 命令行安装开启对方的终端服务	173
6.2 木马	174
6.2.1 木马和后门的区别	174
6.2.2 常见木马的使用	174
6.3 网络代理跳板	177
6.3.1 网络代理跳板的作用	177
6.3.2 网络代理跳板工具的使用	177
6.4 清除日志	181
6.4.1 清除 IIS 日志	182
6.4.2 清除主机日志	183
小结	192
课后习题	192
第 7 章 恶意代码分析与防治	194
7.1 恶意代码概述	194
7.1.1 研究恶意代码的必要性	194
7.1.2 恶意代码的发展史	194
7.1.3 恶意代码长期存在的原因	196
7.2 恶意代码实现机理	196

7.2.1 恶意代码的定义	196
7.2.2 恶意代码攻击机制	197
7.3 恶意代码实现关键技术	198
7.3.1 恶意代码生存技术	198
7.3.2 恶意代码攻击技术	200
7.3.3 恶意代码的隐蔽技术	201
7.4 网络蠕虫	203
7.4.1 网络蠕虫的定义	203
7.4.2 蠕虫的结构	203
7.5 恶意代码防范方法	204
7.5.1 基于主机的恶意代码防范方法	204
7.5.2 基于网络的恶意代码防范方法	206
小结	207
课后习题	207

第三部分 网络安全的防御技术

第8章 安全操作系统基础	211
8.1 常用操作系统概述	211
8.1.1 UNIX 操作系统	211
8.1.2 Linux 操作系统	212
8.1.3 Windows 操作系统	213
8.2 安全操作系统的研究发展	214
8.2.1 国外安全操作系统的发展	214
8.2.2 国内安全操作系统的发展	217
8.3 安全操作系统的基本概念	218
8.3.1 主体和客体	218
8.3.2 安全策略和安全模型	218
8.3.3 访问监控器和安全内核	219
8.3.4 可信计算基	220
8.4 安全操作系统的机制	221
8.4.1 硬件安全机制	221
8.4.2 标识与鉴别	221
8.4.3 访问控制	222
8.4.4 最小特权管理	222
8.4.5 可信通路	223
8.4.6 安全审计	223
8.5 代表性的安全模型	223
8.5.1 安全模型的特点	223
8.5.2 主要安全模型介绍	224
8.6 操作系统安全体系结构	225
8.6.1 安全体系结构的含义	226
8.6.2 安全体系结构的类型	226

8.6.3	Flask 安全体系结构	226
8.6.4	权能体系结构	227
8.7	操作系统安全配置方案	228
8.7.1	安全配置方案初级篇	228
8.7.2	安全配置方案中级篇	230
8.7.3	安全配置方案高级篇	235
小结		244
课后习题		244
第 9 章	密码学与信息加密	246
9.1	密码学概述	246
9.1.1	密码学的发展	246
9.1.2	密码技术简介	247
9.1.3	消息和加密	247
9.1.4	鉴别、完整性和抗抵赖性	248
9.1.5	算法和密钥	248
9.1.6	对称算法	249
9.1.7	公开密钥算法	249
9.2	DES 对称加密技术	249
9.2.1	DES 算法的历史	250
9.2.2	DES 算法的安全性	250
9.2.3	DES 算法的原理	250
9.2.4	DES 算法的实现步骤	251
9.2.5	DES 算法的应用误区	255
9.2.6	DES 算法的程序实现	255
9.3	RSA 公钥加密技术	261
9.3.1	RSA 算法的原理	261
9.3.2	RSA 算法的安全性	261
9.3.3	RSA 算法的速度	261
9.3.4	RSA 算法的程序实现	262
9.4	PGP 加密技术	265
9.4.1	PGP 简介	265
9.4.2	PGP 加密软件	265
9.5	数字信封和数字签名	268
9.5.1	数字签名的原理	268
9.5.2	数字签名的应用例子	269
9.6	数字水印	270
9.6.1	数字水印产生背景	270
9.6.2	数字水印的嵌入方法	271
9.7	公钥基础设施 PKI	271
9.7.1	PKI 的组成	272
9.7.2	PKI 证书与密钥管理	272
9.7.3	PKI 的信任模型	273
小结		273

课后习题	274
第 10 章 防火墙与入侵检测	276
10.1 防火墙的概念	276
10.1.1 防火墙的功能	277
10.1.2 防火墙的必要性	277
10.1.3 防火墙的局限性	277
10.2 防火墙的分类	277
10.2.1 分组过滤防火墙	278
10.2.2 应用代理防火墙	284
10.3 常见防火墙系统模型	285
10.3.1 筛选路由器模型	285
10.3.2 单宿主堡垒主机模型	286
10.3.3 双宿主堡垒主机模型	286
10.3.4 屏蔽子网模型	287
10.4 创建防火墙的步骤	287
10.4.1 制定安全策略	287
10.4.2 搭建安全体系结构	288
10.4.3 制定规则次序	288
10.4.4 落实规则集	288
10.4.5 更换控制	288
10.4.6 审计工作	289
10.5 入侵检测系统的概念	289
10.5.1 入侵检测系统面临的挑战	289
10.5.2 入侵检测系统的类型和性能比较	290
10.6 入侵检测的方法	290
10.6.1 静态配置分析	290
10.6.2 异常性检测方法	290
10.6.3 基于行为的检测方法	291
10.7 入侵检测的步骤	296
10.7.1 信息收集	296
10.7.2 数据分析	296
10.7.3 响应	297
小结	300
课后习题	300
第 11 章 IP 安全与 Web 安全	302
11.1 IP 安全概述	302
11.1.1 IP 安全的必要性	302
11.1.2 IPSec 的实现方式	303
11.1.3 IPSec 的实施	303
11.1.4 验证头 AH	304
11.1.5 封装安全有效载荷 ESP	304
11.2 密钥交换协议 IKE	305

11.2.1 IKE 协议的组成	305
11.2.2 ISAKMP 协议	305
11.2.3 IKE 的两个阶段	306
11.3 VPN 技术	307
11.3.1 VPN 的功能	307
11.3.2 VPN 的解决方案	307
11.4 Web 安全概述	308
11.4.1 网络层安全性	308
11.4.2 传输层安全性	308
11.4.3 应用层安全性	308
11.5 SSL/TLS 技术	309
11.5.1 SSL/TLS 的发展过程	309
11.5.2 SSL 体系结构	310
11.5.3 SSL 的会话与连接	310
11.5.4 OpenSSL 概述	311
11.6 安全电子交易 SET 简介	311
小结	311
课后习题	311

第四部分 网络安全综合解决方案

第 12 章 网络安全方案设计	315
12.1 网络安全方案概念	315
12.1.1 网络安全方案设计的注意点	315
12.1.2 评价网络安全方案的质量	316
12.2 网络安全方案的框架	316
12.3 网络安全案例需求	318
12.3.1 项目要求	318
12.3.2 工作任务	319
12.4 解决方案设计	319
12.4.1 公司背景简介	319
12.4.2 安全风险分析	320
12.4.3 解决方案	321
12.4.4 实施方案	321
12.4.5 技术支持	322
12.4.6 产品报价	322
12.4.7 产品介绍	322
12.4.8 第三方检测报告	322
12.4.9 安全技术培训	322
小结	324
课后习题	324
附录 A 部分习题参考答案	325
参考文献	329

第一部分

计算机网络安全基础

本部分包括：

★第1章 网络安全概述与环境配置

- ☒ 网络安全研究的体系、研究网络安全的必要性
- ☒ 研究网络安全的社会意义,与网络安全有关的法规
- ☒ 评价一个系统或者应用软件的安全等级
- ☒ 较为详细地介绍实验环境的配置

★第2章 网络安全协议基础

- ☒ OSI 七层网络模型、TCP/IP 协议族
- ☒ IP 协议、TCP 协议、UDP 协议和 ICMP 协议
- ☒ 常用的网络服务:FTP 服务、Telnet 服务等
- ☒ 常用的网络服务端口和常用的网络命令

★第3章 网络安全编程基础

- ☒ 操作系统编程中的 C 和 C++ 语言
- ☒ C 语言的 4 个发展阶段
- ☒ Socket 编程、注册表编程
- ☒ 定时器编程、驻留程序编程和多线程编程

第 1 章 网络安全概述与环境配置

本章要点

- ☑ 介绍网络安全研究的体系、研究网络安全的必要性
- ☑ 研究网络安全的社会意义,目前与计算机网络安全有关的法规
- ☑ 评价一个系统或者应用软件的安全等级
- ☑ 详细介绍实验环境的配置

1.1 信息安全概述

网络安全是信息安全学科的重要组成部分。信息安全是一门交叉学科,广义上讲,信息安全涉及多方面的理论和应用知识,除了数学、通信、计算机等自然科学外,还涉及法律、心理学等社会科学。狭义上讲,也就是通常说的信息安全,只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

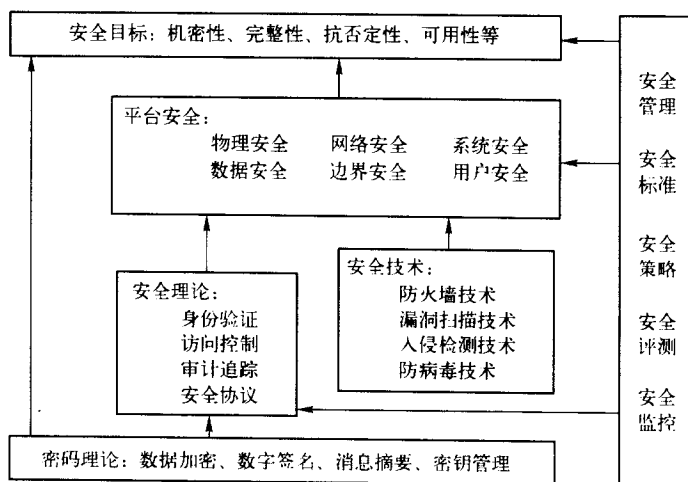


图 1-1 信息安全研究内容及关系

信息安全研究大致可以分为基础理论研究、应用技术研究、安全管理研究等。基础研究包括密码研究、安全理论研究；应用技术研究则包括安全实现技术、安全平台技术研究；安全管理研究包括安全标准、安全策略、安全测评等。

1.1.1 信息安全研究层次

信息安全从总体上可以分成 5 个层次：安全的密码算法、安全协议、网络安全、系统安全和