

高等学校计算机科学与技术教材

信息安全概论

石志国 贺也平 赵悦 编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

本书系统介绍了信息安全学科的内容。本书与同类书籍相比,大大提高了实践部分的比例,全书理论与实践的比例约为6:4,并引用大量的经典例子,注重提高学习信息安全的趣味性与知识性及授课的生动性。

全书从信息安全研究层次角度分成4部分,共11章。第一部分:信息安全基础,介绍信息安全学的基本概念及安全的评价标准。第二部分:密码学基础,介绍信息加密与密码分析、认证及密钥管理技术。第三部分:网络安全技术,介绍PKI公钥基础设施原理、防火墙与入侵检测技术、IP安全与Web安全,以及简单介绍了典型攻击技术。第四部分:系统与应用安全技术,介绍安全操作系统理论、恶意代码与病毒机制、可信计算的基本概念及信息安全法律与法规。

本书可作为高等学校和各类培训机构相关课程的教材或参考书。本书提供全书源代码,以及涉及的所有软件和授课幻灯片等教学支持信息,读者可以从图书支持网站<http://www.gettop.net>下载,也可以从北京交通大学出版社网站<http://press.bjtu.edu.cn>的下载栏目中下载。

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。

版权所有,侵权必究。侵权举报电话:010-62782989 13501256678 13801310933

图书在版编目(CIP)数据

信息安全概论/石志国,贺也平,赵悦编著. —北京:清华大学出版社;北京交通大学出版社,2007.6

(高等学校计算机科学与技术教材)

ISBN 978-7-81082-998-4

I. 信... II. ①石... ②贺... ③赵... III. 信息系统-安全技术-高等学校-教材
IV. TP309

中国版本图书馆CIP数据核字(2007)第056547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:18 字数:458千字

版 次:2007年6月第1版 2007年6月第1次印刷

书 号:ISBN 978-7-81082-998-4/TP·348

印 数:5000册 定价:29.00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@bjtu.edu.cn。

前 言

信息安全学是一门新兴的学科,2004年成为一门正式的本科专业,目前已经成为很多科研机构和大专院校的一个重要研究领域。信息安全概论需要全面阐述该学科目前的发展层次,研究内容和最新的发展方向。本书对信息安全学科内容进行整体介绍,根据信息安全学目前最新发展重新规划学科的内容及各部分比重。

信息安全学是一门实践性很强的学科,本书除了对相关理论进行全面讲解外,还通过具体的实验、例子等更加具体形象地化解理论的枯燥和繁杂。本书的整体定位是教材,书后提供大量习题,因此也可以同时作为相关考试的参考书。为了方便使用,提高质量,本书提供完整的教学大纲及教案等辅助资料。

目前很多信息安全教程理论性很强,这样接受起来相对比较困难。本书把理论知识和实验实践结合讲解,注重提高学习信息安全的趣味性与知识性,以及授课的生动性。

全书从信息安全研究层次角度分成4部分,共11章。

第一部分 信息安全基础

第1章 信息安全概述:介绍信息安全的学科内容、研究层次及安全威胁。研究信息安全的社会意义,相关道德标准及黑客行为学研究内容。

第二部分 密码学基础

第2章 信息加密与密码分析:介绍密码学的基本概念、加密类型,混合加密方法以及消息一致性。并介绍加密领域中两种主流加密技术:DES加密和RSA加密。

第3章 认证与密钥管理技术:介绍哈希函数的分类与MD5的基本算法、常用的身份识别技术、电子ID身份识别和个人特征身份识别,以及密钥管理技术与管理系统。

第三部分 网络安全技术

第4章 PKI公钥基础设施原理:介绍PKI/CA模型的构成、RSA算法在PKI/CA中的应用、PKI策略、PKI的规划和建设,以及CA的应用。

第5章 防火墙与入侵检测技术: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6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以及VPN的解决方案等。

第7章 典型攻击技术简介:介绍常用的网络入侵技术,包括社会工程学攻击、物理攻击、暴力攻击、漏洞攻击及缓冲区溢出攻击等。

第四部分 系统与应用安全技术

第8章 安全操作系统:介绍安全操作系统的基本概念、实现机制,安全模型及安全体系结构。

第9章 恶意代码与病毒: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

此为试读,需要完整PDF请访问:www.ertongbook.com

码实现机理、定义及攻击方法等。

第 10 章 可信计算简介 :介绍可信计算的发展历史、可信计算的设计目标、可以计算的基本规范、可信计算中使用的密钥和信任状、平台配置寄存器 PCR 的原理及可信计算中信任状验证方式

第 11 章 信息安全法律法规与管理 :介绍世界范围内的信息安全法规内容、国际相关法律法规现状与特点、相关政策法规的现状与特点 ,部分相关法律法规简介、立法方面存在的问题及信息安全犯罪案例分析。

总的来说 ,本书具有如下的特点。

(1) 注重培养理论水平和实践能力。针对所讲述的理论知识提供直观的试验或者实例 ,涉及的实例或者试验 ,都具有很高的实用价值。

(2) 总体上讲解信息安全的层次。适应目前计算机教学的需要。并对重要知识点进行详细的讲解 ,使之成为一本适合教学和自学的图书 ,本书浅显易懂、循序渐进、适合教学的需要。

(3) 每章提供本章要点 ,小结。并全面地提供课后习题。习题包括 选择、填空、简答题和程序设计题目等 ,并在书后给出部分习题答案。

在本书的编写过程中 ,得到众多老师的指导和帮助。在此感谢中科院软件所卿斯汉研究员、淮晓永副教授、程光瑶老师、蒋建春老师、周辉老师、于文卫老师、张东帆老师、王秀利老师、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、尹浩副教授 ,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、田萧老师和王春凤老师 ,感谢中国软件行业协会邱钦伦高级工程师。尤其要感谢的是北京交通大学出版社的编辑谭文芳老师 ,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。

本书可以作为高等学校和各类培训机构相关课程的教材或者教学参考书 ,也可作为信息安全自学人员和信息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 5 月

目 录

第一部分 信息安全基础

| | |
|------------------------|----|
| 第 1 章 信息安全概述 | 2 |
| 1.1 信息的概念 | 2 |
| 1.1.1 信息的定义 | 2 |
| 1.1.2 信息的概念 | 2 |
| 1.2 信息的概念 | 3 |
| 1.2.1 信息安全学科内容 | 3 |
| 1.2.2 信息安全研究层次 | 5 |
| 1.2.3 信息安全的发展 | 6 |
| 1.2.4 信息的威胁 | 6 |
| 1.3 研究信息安全的意义 | 7 |
| 1.3.1 信息安全与政治 | 8 |
| 1.3.2 信息安全与经济 | 8 |
| 1.3.3 信息安全与社会稳定 | 8 |
| 1.3.4 信息安全与军事 | 9 |
| 1.4 信息的威胁者——黑客概述 | 9 |
| 1.4.1 什么是黑客 | 9 |
| 1.4.2 黑客简史 | 9 |
| 1.4.3 中国黑客的发展 | 12 |
| 1.4.4 黑客的行为特征 | 13 |
| 1.4.5 知名黑客介绍 | 13 |
| 1.5 信息的评价标准 | 14 |
| 1.5.1 我国评价标准 | 14 |
| 1.5.2 美国国防部评价标准 | 14 |
| 1.5.3 欧洲评价标准 | 16 |
| 1.5.4 通用评价准则 | 16 |
| 1.5.5 评估标准间的关系 | 17 |
| 小结 | 17 |
| 课后习题 | 17 |

第二部分 密码学基础

| | |
|-----------------------|----|
| 第 2 章 信息加密与密码分析 | 20 |
|-----------------------|----|

| | | |
|-------|----------------------|----|
| 2.1 | 密码学概述..... | 20 |
| 2.1.1 | 密码学的发展..... | 20 |
| 2.1.2 | 密码技术简介..... | 21 |
| 2.1.3 | 消息和加密..... | 21 |
| 2.1.4 | 鉴别、完整性和抗抵赖性 | 22 |
| 2.1.5 | 算法和密钥..... | 22 |
| 2.1.6 | 对称算法..... | 23 |
| 2.1.7 | 公开密钥算法..... | 23 |
| 2.2 | 加密类型简介..... | 23 |
| 2.2.1 | scytale 密码和凯撒密码..... | 23 |
| 2.2.2 | 代替密码和置换密码..... | 24 |
| 2.2.3 | 转轮机..... | 26 |
| 2.2.4 | 一次一密乱码本..... | 28 |
| 2.2.5 | 对称和非对称算法..... | 29 |
| 2.2.6 | 分组密码和序列密码..... | 30 |
| 2.2.7 | 流密码简介..... | 30 |
| 2.3 | 常用加密算法简介..... | 31 |
| 2.3.1 | IDEA 算法 | 31 |
| 2.3.2 | AES 算法 | 31 |
| 2.3.3 | RC5 算法 | 32 |
| 2.3.4 | RC4 序列算法 | 33 |
| 2.3.5 | 椭圆曲线算法..... | 33 |
| 2.4 | DES 对称加密技术 | 34 |
| 2.4.1 | DES 算法的历史 | 34 |
| 2.4.2 | DES 算法的安全性 | 35 |
| 2.4.3 | DES 算法的原理 | 35 |
| 2.4.4 | DES 算法的实现步骤 | 36 |
| 2.4.5 | DES 算法的应用误区 | 40 |
| 2.4.6 | DES 算法的程序实现 | 41 |
| 2.5 | RSA 公钥加密技术 | 46 |
| 2.5.1 | RSA 算法的原理 | 46 |
| 2.5.2 | RSA 算法的安全性 | 47 |
| 2.5.3 | RSA 算法的速度 | 47 |
| 2.5.4 | RSA 算法的程序实现 | 47 |
| 2.6 | 密码分析与攻击..... | 51 |
| 2.6.1 | 典型的攻击方法..... | 51 |
| 2.6.2 | 算法攻击举例..... | 52 |
| 2.7 | 密码学应用..... | 55 |
| 2.7.1 | 密码应用模式..... | 55 |

| | | |
|--------|--------------------|----|
| 2.7.2 | 加密方式..... | 57 |
| 2.7.3 | 加密和验证协议..... | 58 |
| 2.8 | PGP 加密技术应用 | 61 |
| 2.8.1 | PGP 简介 | 61 |
| 2.8.2 | PGP 加密软件 | 61 |
| | 小结 | 66 |
| | 课后习题 | 66 |
| 第 3 章 | 认证与密钥管理技术 | 68 |
| 3.1 | 哈希函数..... | 68 |
| 3.2 | 身份识别技术 | 69 |
| 3.2.1 | 电子 ID 身份识别技术 | 69 |
| 3.2.2 | 个人特征的身份证明..... | 70 |
| 3.3 | 基于零知识证明的识别技术 | 71 |
| 3.4 | 密钥管理技术..... | 72 |
| 3.4.1 | 对称密钥的管理..... | 72 |
| 3.4.2 | 非对称密钥的管理..... | 73 |
| 3.5 | 密钥管理系统..... | 74 |
| 3.5.1 | 密钥的分配..... | 74 |
| 3.5.2 | 计算机网络密钥分配方法..... | 75 |
| 3.5.3 | 密钥注入..... | 76 |
| 3.5.4 | 密钥存储..... | 76 |
| 3.5.5 | 密钥更换和密钥吊销..... | 76 |
| 3.6 | 密钥产生技术..... | 77 |
| 3.6.1 | 密钥产生的硬件技术 | 77 |
| 3.6.2 | 密钥产生的软件技术 | 77 |
| 3.7 | 密钥的分散管理与托管..... | 78 |
| 3.7.1 | 密钥的分散、分配和分发 | 79 |
| 3.7.2 | 密钥的托管技术..... | 79 |
| 3.7.3 | 部分密钥托管技术..... | 81 |
| 3.8 | 消息一致性和数字签名..... | 81 |
| 3.8.1 | 消息一致性..... | 81 |
| 3.8.2 | 数字签名..... | 82 |
| 3.8.3 | 数字签名的应用例子..... | 84 |
| 3.9 | 信息隐藏概述..... | 85 |
| 3.9.1 | 信息隐藏的历史..... | 85 |
| 3.9.2 | 信息隐藏的研究内容..... | 86 |
| 3.10 | 信息隐藏基本原理 | 87 |
| 3.10.1 | 无密钥信息隐藏 | 87 |
| 3.10.2 | 私钥信息隐藏 | 87 |

| | |
|------------------------|----|
| 3.10.3 公钥信息隐藏 | 88 |
| 3.11 数字水印 | 88 |
| 3.11.1 数字水印产生背景 | 88 |
| 3.11.2 数字水印的嵌入方法 | 89 |
| 小结 | 90 |
| 课后习题 | 90 |

第三部分 网络安全技术

| | |
|----------------------------|-----|
| 第4章 PKI 公钥基础设施原理 | 94 |
| 4.1 PKI/CA 模型 | 94 |
| 4.1.1 PKI 简介 | 94 |
| 4.1.2 PKI/CA 模型的构成 | 95 |
| 4.1.3 PKI 的其他元素 | 96 |
| 4.1.4 PKI 的基本功能 | 96 |
| 4.2 PKI 策略 | 97 |
| 4.2.1 认证机构的策略 | 97 |
| 4.2.2 证书中心架构分类 | 99 |
| 4.2.3 认证机构具体组成 | 100 |
| 4.2.4 认证机构密钥管理 | 102 |
| 4.3 PKI 的规划和建设 | 109 |
| 4.3.1 美国 PKI 规划情况 | 109 |
| 4.3.2 加拿大政府 PKI 体系结构 | 112 |
| 4.3.3 两种体系的比较 | 112 |
| 4.3.4 我国的 PKI 发展规划 | 113 |
| 4.3.5 我国的 PKI 体系建设情况 | 114 |
| 小结 | 116 |
| 课后习题 | 116 |
| 第5章 防火墙与入侵检测技术 | 118 |
| 5.1 防火墙的概念 | 118 |
| 5.1.1 防火墙的功能 | 119 |
| 5.1.2 防火墙的必要性 | 119 |
| 5.1.3 防火墙的局限性 | 119 |
| 5.2 防火墙的分类 | 119 |
| 5.2.1 分组过滤防火墙 | 120 |
| 5.2.2 应用代理防火墙 | 127 |
| 5.3 常见防火墙系统模型 | 128 |
| 5.3.1 筛选路由器模型 | 128 |
| 5.3.2 单宿主堡垒主机模型 | 128 |
| 5.3.3 双宿主堡垒主机模型 | 129 |

| | | |
|-------|----------------------|-----|
| 5.3.4 | 屏蔽子网模型 | 129 |
| 5.4 | 创建防火墙的步骤 | 130 |
| 5.4.1 | 制定安全策略 | 130 |
| 5.4.2 | 搭建安全体系结构 | 130 |
| 5.4.3 | 制定规则次序 | 130 |
| 5.4.4 | 落实规则集 | 131 |
| 5.4.5 | 更换控制 | 131 |
| 5.4.6 | 审计工作 | 131 |
| 5.5 | 入侵检测系统的概念 | 132 |
| 5.5.1 | 入侵检测系统面临的挑战 | 132 |
| 5.5.2 | 入侵检测系统的类型和性能比较 | 133 |
| 5.6 | 入侵检测的方法 | 133 |
| 5.6.1 | 静态配置分析 | 133 |
| 5.6.2 | 异常性检测方法 | 133 |
| 5.6.3 | 基于行为的检测方法 | 134 |
| 5.7 | 入侵检测的步骤 | 139 |
| 5.7.1 | 信息收集 | 139 |
| 5.7.2 | 数据分析 | 139 |
| 5.7.3 | 响应 | 140 |
| | 小结 | 143 |
| | 课后习题 | 143 |
| 第 6 章 | IP 安全与 Web 安全 | 145 |
| 6.1 | IP 安全概述 | 145 |
| 6.1.1 | IP 安全的必要性 | 145 |
| 6.1.2 | IPSec 的实现方式 | 146 |
| 6.1.3 | IPSec 的实施 | 146 |
| 6.1.4 | 验证头 AH | 147 |
| 6.1.5 | 封装安全有效载荷 ESP | 147 |
| 6.2 | 因特网密钥交换协议 IKE | 148 |
| 6.2.1 | IKE 协议的组成 | 148 |
| 6.2.2 | ISAKMP 协议 | 148 |
| 6.2.3 | IKE 的两个阶段 | 149 |
| 6.3 | VPN 技术 | 150 |
| 6.3.1 | VPN 的功能 | 150 |
| 6.3.2 | VPN 的解决方案 | 150 |
| 6.4 | Web 安全概述 | 151 |
| 6.4.1 | 网络层安全性 | 151 |
| 6.4.2 | 传输层安全性 | 151 |
| 6.4.3 | 应用层安全性 | 151 |

| | | |
|-------|-------------------------|-----|
| 6.5 | SSL/TLS 技术 | 152 |
| 6.5.1 | SSL/TLS 的发展过程 | 152 |
| 6.5.2 | SSL 体系结构 | 152 |
| 6.5.3 | SSL 的会话与连接 | 153 |
| 6.5.4 | OpenSSL 概述 | 154 |
| 6.6 | SET 协议简介 | 154 |
| | 小结 | 154 |
| | 课后习题 | 154 |
| 第 7 章 | 典型攻击技术简介 | 156 |
| 7.1 | 社会工程学攻击 | 156 |
| 7.2 | 物理攻击与防范 | 157 |
| 7.2.1 | 获取管理员密码 | 157 |
| 7.2.2 | 权限提升 | 158 |
| 7.3 | 暴力攻击 | 160 |
| 7.3.1 | 字典文件 | 160 |
| 7.3.2 | 暴力破解操作系统密码 | 160 |
| 7.3.3 | 暴力破解邮箱密码 | 161 |
| 7.3.4 | 暴力破解软件密码 | 162 |
| 7.4 | Unicode 漏洞专题 | 164 |
| 7.4.1 | Unicode 漏洞的检测方法 | 164 |
| 7.4.2 | 使用 Unicode 漏洞进行攻击 | 167 |
| 7.5 | 其他漏洞攻击 | 170 |
| 7.5.1 | 利用打印漏洞 | 170 |
| 7.5.2 | SMB 致命攻击 | 171 |
| 7.6 | 缓冲区溢出攻击 | 172 |
| 7.6.1 | RPC 漏洞溢出 | 172 |
| 7.6.2 | 利用 IIS 溢出进行攻击 | 174 |
| 7.6.3 | 利用 WebDav 远程溢出 | 176 |
| 7.7 | 拒绝服务攻击 | 181 |
| 7.7.1 | SYN 风暴 | 181 |
| 7.7.2 | Smurf 攻击 | 183 |
| 7.7.3 | 利用处理程序错误进行攻击 | 185 |
| 7.8 | 分布式拒绝服务攻击 | 185 |
| 7.8.1 | DDoS 的特点 | 186 |
| 7.8.2 | 攻击手段 | 186 |
| 7.8.3 | DDoS 的著名攻击工具 | 186 |
| 7.8.4 | 拒绝服务攻击的发展趋势 | 188 |
| 7.9 | 防范拒绝服务攻击 | 188 |
| | 小结 | 189 |

| | |
|-----------|-----|
| 课后习题..... | 189 |
|-----------|-----|

第四部分 系统与应用安全技术

| | |
|--------------------------|-----|
| 第8章 安全操作系统..... | 192 |
| 8.1 常用操作系统概述 | 192 |
| 8.1.1 UNIX 操作系统 | 192 |
| 8.1.2 Linux 操作系统 | 193 |
| 8.1.3 Windows 操作系统 | 195 |
| 8.2 安全操作系统的研究发展 | 195 |
| 8.2.1 国外安全操作系统的发展 | 195 |
| 8.2.2 国内安全操作系统的发展 | 198 |
| 8.3 安全操作系统的基本概念 | 199 |
| 8.3.1 主体和客体 | 199 |
| 8.3.2 安全策略和安全模型 | 200 |
| 8.3.3 访问监控器和安全内核 | 200 |
| 8.3.4 可信计算基 | 201 |
| 8.4 安全操作系统的机制 | 202 |
| 8.4.1 硬件安全机制 | 202 |
| 8.4.2 标识与鉴别 | 203 |
| 8.4.3 访问控制 | 203 |
| 8.4.4 最小特权管理 | 204 |
| 8.4.5 可信通路 | 204 |
| 8.4.6 安全审计 | 204 |
| 8.5 代表性的安全模型 | 205 |
| 8.5.1 安全模型的特点 | 205 |
| 8.5.2 主要安全模型介绍 | 205 |
| 8.6 操作系统安全体系结构 | 207 |
| 8.6.1 安全体系结构的含义 | 207 |
| 8.6.2 安全体系结构的类型 | 207 |
| 8.6.3 Flask 安全体系结构 | 208 |
| 8.6.4 权能体系结构 | 209 |
| 小结..... | 209 |
| 课后习题..... | 209 |
| 第9章 恶意代码与病毒..... | 211 |
| 9.1 恶意代码概述 | 211 |
| 9.1.1 研究恶意代码的必要性 | 211 |
| 9.1.2 恶意代码的发展史 | 211 |
| 9.1.3 恶意代码长期存在的原因 | 213 |
| 9.2 恶意代码的实现机理 | 213 |

| | | |
|--------|---------------------------|-----|
| 9.2.1 | 恶意代码的定义 | 213 |
| 9.2.2 | 恶意代码的攻击机制 | 214 |
| 9.3 | 实现恶意代码的关键技术 | 215 |
| 9.3.1 | 恶意代码的生存技术 | 215 |
| 9.3.2 | 恶意代码的攻击技术 | 217 |
| 9.3.3 | 恶意代码的隐蔽技术 | 218 |
| 9.4 | 网络蠕虫 | 220 |
| 9.4.1 | 网络蠕虫的定义 | 220 |
| 9.4.2 | 蠕虫的结构 | 220 |
| 9.5 | 恶意代码防范方法 | 221 |
| 9.5.1 | 基于主机的恶意代码防范方法 | 222 |
| 9.5.2 | 基于网络的恶意代码防范方法 | 223 |
| | 小结..... | 225 |
| | 课后习题..... | 225 |
| 第 10 章 | 可信计算简介 | 227 |
| 10.1 | 可信计算概述..... | 227 |
| 10.1.1 | 可信计算的发展历史..... | 227 |
| 10.1.2 | 可信计算的目标..... | 228 |
| 10.1.3 | 可信计算的基本规范..... | 229 |
| 10.1.4 | 可信计算的密钥和信任状..... | 230 |
| 10.2 | 可信计算中的验证机制..... | 231 |
| 10.2.1 | 平台配置寄存器..... | 232 |
| 10.2.2 | 平台密钥与检测过程..... | 232 |
| 10.2.3 | 信任状验证方式..... | 233 |
| | 小结..... | 234 |
| | 课后习题..... | 234 |
| 第 11 章 | 信息安全法律法规与管理 | 235 |
| 11.1 | 信息安全相关法律法规现状..... | 235 |
| 11.1.1 | 美国计算机犯罪立法..... | 235 |
| 11.1.2 | 英国计算机犯罪法..... | 237 |
| 11.1.3 | 德国计算机犯罪法..... | 238 |
| 11.1.4 | 法律法规的特点及现状..... | 239 |
| 11.2 | 我国政策法规的现状特点..... | 239 |
| 11.3 | 部分相关法律法规简介..... | 241 |
| 11.3.1 | 国际联网管理..... | 241 |
| 11.3.2 | 商用密码管理..... | 243 |
| 11.3.3 | 计算机病毒防治..... | 244 |
| 11.3.4 | 安全产品检测与销售..... | 244 |
| 11.3.5 | 中国人民解放军计算机信息系统安全保密规定..... | 244 |

| | | |
|---------|------------------------------|-----|
| 11.4 | 刑法中规定的信息安全犯罪..... | 245 |
| 11.4.1 | 非法侵入计算机信息系统罪..... | 245 |
| 11.4.2 | 破坏计算机信息系统罪..... | 247 |
| 11.4.3 | 利用计算机实施的金融犯罪..... | 248 |
| 11.4.4 | 传授犯罪方法罪..... | 249 |
| 11.4.5 | 破坏通信设备罪..... | 249 |
| 11.4.6 | 其他计算机犯罪..... | 250 |
| 11.5 | 信息安全相关的民事责任..... | 251 |
| 11.5.1 | 计算机软件的法律保护及法律责任..... | 251 |
| 11.5.2 | 电子出版物的法律保护..... | 251 |
| 11.5.3 | 计算机软件的商业秘密和竞争的法律保护及法律责任..... | 251 |
| 11.5.4 | 电子公告服务相关的法律管制..... | 253 |
| 11.6 | 立法方面存在的问题..... | 254 |
| 11.6.1 | 内容重复交叉..... | 254 |
| 11.6.2 | 同一行为有多个行政处罚主体..... | 254 |
| 11.6.3 | 引用法律不当..... | 255 |
| 11.6.4 | 违法设定行政处罚的种类..... | 255 |
| 11.6.5 | 规章与行政法规相抵触..... | 255 |
| 11.6.6 | 处罚幅度不一致..... | 255 |
| 11.6.7 | 行政审批部门及审批事项多..... | 256 |
| 11.7 | 信息安全犯罪案例分析..... | 256 |
| 11.7.1 | 电子邮件犯罪..... | 256 |
| 11.7.2 | 对电子邮件取证..... | 257 |
| 11.8 | 计算机犯罪调查..... | 257 |
| 11.8.1 | 计算机犯罪基本定义..... | 257 |
| 11.8.2 | 狭义和广义计算机犯罪..... | 258 |
| 11.8.3 | 纯正和不纯正计算机犯罪..... | 259 |
| 11.8.4 | 计算机犯罪特点..... | 260 |
| 11.8.5 | 犯罪共性..... | 260 |
| 11.9 | 计算机犯罪的发展趋势..... | 262 |
| 11.9.1 | 宏观发展趋势..... | 262 |
| 11.9.2 | 计算机犯罪的自身发展趋势..... | 263 |
| 11.9.3 | 计算机犯罪具体形式及危害..... | 263 |
| 11.10 | 计算机犯罪的预防..... | 264 |
| 11.10.1 | 安全环境..... | 264 |
| 11.10.2 | 使用加密技术..... | 265 |
| 11.10.3 | 软件加密..... | 265 |
| 11.10.4 | 口令加密..... | 265 |
| 11.10.5 | 审计..... | 265 |

| | |
|---------------------|-----|
| 11.10.6 硬件投资 | 265 |
| 11.10.7 计算机取证 | 265 |
| 11.11 信息安全管理 | 267 |
| 小结..... | 267 |
| 课后习题..... | 267 |
| 附录 A 部分习题参考答案..... | 269 |
| 参考文献..... | 272 |

第一部分

信息安全基础

第 1 章 信息安全概述

本章要点

- ✎ 信息的定义和信息技术的研究内容
 - ✎ 信息安全的学科内容、研究层次和安全威胁
 - ✎ 研究信息安全的社会意义、相关道德标准和黑客行为学研究内容
 - ✎ 信息安全评价标准
-

1.1 信息技术的概念

信息是人类社会必需的重要资源,信息安全是社会安全稳定条件的必要条件。信息是一切生物进化的导向资源,信息是知识的来源、是决策的依据、是控制的灵魂、是思维的材料、是管理的基础。

1.1.1 信息的定义

信息是一种以特殊的物质形态存在的实体,1928年哈特莱(L. V. R. Hartley)认为信息是选择通信符号的方式,且用选择自由度来计量这种信息的大小。1948年,美国数学家香农(C. E. Shannon)认为信息是用来减少随机不定性的东西。1948年,维纳(N. Wiener)认为信息是人们在适应外部世界和这种适应反作用于外部世界的过程中,与外部世界进行互相交换的内容的名称。1975年,意大利学者朗高(G. Longo)认为信息反映了事物的形式、关系和差别,它包含在事物的差异之中,而不在事物本身。1988年,我国信息论专家钟义信教授在《信息科学原理》一书中,把信息定义为事物的运动状态和状态变化的方式,并通过引入约束条件推导了信息的概念体系,对信息进行了完整和准确的描述。

信息不同于消息,消息是信息的外壳,信息则是消息的内核。信息不同于信号,信号是信息的载体,信息则是信号所载荷的内容。信息不同于数据,数据是记录信息的一种形式,同样的信息也可以用文字或图像来表述。当然,在计算机里,所有的多媒体文件都是用数据表示的,计算机和网络上传递都是以数据的形式进行,此时信息等同于数据。

信息最基本的特征是信息来源于物质,又不是物质本身;它从物质的运动中产生出来,又可以脱离源物质而寄生于媒体物质,相对独立地存在。信息是具体的,并且可以被(生物、机器等)所感知、提取、识别,可以被传递、储存、变换、处理、显示检索和利用。信息的基本功能在于维持和强化世界的有序性,维系着社会的生存,促进人类文明的进步和人类自身的发展。

1.1.2 信息技术的概念

人类的一切活动都可以归结为认识世界和改造世界。从信息的观点来看,人类认识世界

和改造世界的过程,就是一个不断从外部世界的客体中获取信息,并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出,最终把大脑中产生的决策信息反作用于外部世界的过程。现代(大体从 20 世纪中期算起)人类所利用的表征性资源是信息资源,表征性的科学技术是信息科学技术,表征性的工具是智能工具。

信息技术(Information Technology)是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频及语音信息,并且包括提供设备和信息服务两大方面的方法与设备的总称。也有人认为信息技术简单地说就是 3C,Computer(计算机)、Communication(通信)和 Control(控制),即 IT = Computer + Communication + Control。

1.2 信息安全的概念

信息安全学关注信息本身的安全,而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产,以防止偶然的或未授权者对信息的恶意泄露、修改和破坏,从而导致信息的不可靠或无法处理等。这样可以使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

信息安全可以分为数据安全和系统安全。信息安全可以分成两个层次。

从消息层次来看,包括信息的完整性(Integrity),即保证消息的来源、去向、内容真实无误;保密性(Confidentiality),即保证消息不会被非法泄露扩散;不可否认性(Non-repudiation),也称为不可抵赖性,即保证消息的发送和接受者无法否认自己所做过的操作行为。

从网络层次来看,包括可用性(Availability),即保证网络和信息系统随时可用,运行过程中不出现故障,若遇意外打击能够尽量减少并尽早恢复正常;可控性(Controllability)是对网络信息的传播及内容具有控制能力的特性。

1.2.1 信息安全学科内容

信息安全是一门交叉学科。广义上,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,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不研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

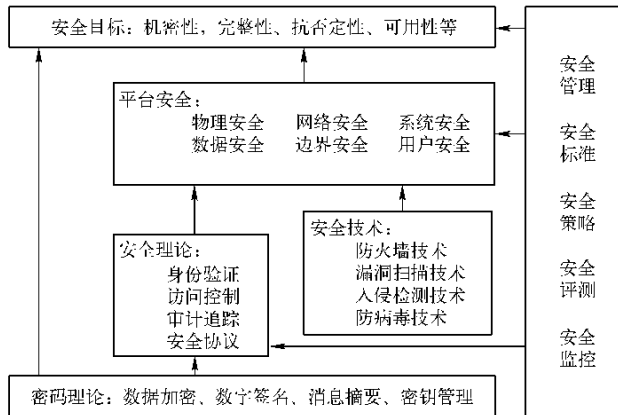


图 1-1 信息安全研究内容及关系