

## <<计算机系统安全>>

### 图书基本信息

书名：<<计算机系统安全>>

13位ISBN编号：9787040133110

10位ISBN编号：7040133113

出版时间：2003-9

出版范围：高等教育

作者：曹天杰

页数：308

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<计算机系统安全>>

### 前言

计算机在政治、军事、金融、商业等部门的应用越来越广泛，社会对计算机网络信息系统的依赖也越来越大，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱，随着全球安全事件的逐年增多，确保网络信息系统的安全已引起世人的关注，信息安全在各国都受到了前所未有的重视。

“9.11”之后，美国联邦调查局所属的关键性基础设施保护中心发布了《关于网络空间安全的国家战略》的报告，明确地将信息安全提升到了关系国家战略的高度，“信息安全+国土安全=国家安全”正逐渐得到社会的认同。

我国正逐步形成一个完善的统一的安全保障体系，成立了国家计算机网络应急处理协调中心（简称CNCERT，<http://www.cen.org.cn/>）、国家计算机病毒应急处理中心（<http://www.tivims.china.org.cn/>）、国家计算机网络入侵防范中心（<http://www.nipc.org.cn/>）、信息安全国家重点实验室（<http://www.is.ac.cn/>）等一批国家级机构。

信息安全、信息对抗、密码学等专业已开始在许多高校及科研院所招生，并开设了“计算机系统安全”、“密码学”等相关课程，但目前我国信息安全人才依然缺乏，内容系统全面反映最新进展的优秀本科信息安全教材还不多见。

## <<计算机系统安全>>

### 内容概要

本书全面系统地介绍了计算机系统安全知识，反映了计算机系统安全领域的新概念、新发展。全书分十三章，涉及了密码学、物理安全、运行安全（风险分析、审计跟踪、备份与恢复、应急）、信息安全（网络安全、访问控制、认证等）等内容。

本书概念准确、选材合理、结构紧凑、条理清晰。书中提供的习题与实验有助于读者进一步深化学习。本书适合计算机科学与技术、信息安全等专业作为“计算机系统安全”、“计算机网络安全”等相关课程的本专科教材，也可作为工程技术人员系统学习信息安全理论的参考书。

## &lt;&lt;计算机系统安全&gt;&gt;

## 书籍目录

第一章 计算机系统安全概述1一、计算机系统安全的概念11、世界范围内日益严重的安全问题12、计算机系统安全的概念23、国内外计算机系统安全标准5二、安全威胁61、安全威胁的种类62、威胁的表现形式8三、安全模型111、P2DR安全模型112、PDRR安全模型14四、风险管理151、风险管理的基本概念152、风险管理的生命周期163、风险管理系统18五、安全体系结构191、安全策略的概念192、安全策略的组成213、安全体系结构22第二章 计算机系统的物理安全28一、环境安全28二、设备安全291、设备安全的保护内容292、TEMPEST技术303、电子战系统32三、媒体安全33第三章 计算机系统的可靠性35一、什么是计算机系统的可靠性35二、容错系统的概念35三、硬件冗余37四、软件冗余40五、磁盘阵列存储器的编码容错方案42第四章 密码学基础47一、密码学概述471、加密和解密472、对称算法和公开密钥算法493、随机序列与随机数514、密码分析525、密码协议54二、传统密码学551、置换密码552、代换密码553、一次一密密码57三、分组密码581、代换-置换网络582、数据加密标准DES603、高级加密标准AES674、工作模式72四、公钥密码751、单向陷门函数752、RSA算法76五、密钥管理79第五章 消息认证与数字签名83一、消息认证831、消息认证方案832、散列函数853、MD5算法87二、数字签名89三、应用：数字水印92第六章 公开密钥基础设施PKI97一、需要解决的问题97二、信任模式与PKI体系结构981、直接信任与第三方信任982、PKI的体系结构1003、CTCA的体系结构101三、证书1031、证书的概念1032、证书格式1043、证书认证系统105第七章 身份认证110一、认证的基本原理1101、身份认证概述1102、口令机制1113、智能卡1124、生物特征认证115二、认证协议1181、基于口令的认证1182、基于对称密码的认证1213、基于公钥密码的认证1234、零知识身份认证125三、典型的认证应用1281、Kerberos认证1282、X.509认证133第八章 访问控制135一、访问控制的概念1351、什么是访问控制1352、访问控制的基本原则136二、自主访问控制(DAC)1371、什么是自主访问控制1372、基于行的自主访问控制1383、基于列的自主访问控制138三、强制访问控制(MAC)139四、基于角色访问控制(RBAC)1401、RBAC的基本思想1402、RBAC描述复杂的安全策略1433、RBAC系统结构144第九章 防火墙146一、防火墙概述146二、网络策略1471、服务访问政策1472、防火墙设计政策148三、防火墙体系结构1481、双重宿主主机体系结构1482、屏蔽主机体系结构1493、屏蔽子网体系结构150四、包过滤技术152五、代理服务技术1551、代理服务概述1552、应用层网关及HTTP代理1583、电路层网关及SOCKS代理159第十章 攻击与应急响应162一、攻击概述1621、攻击的一些基本概念1622、系统的漏洞1633、远程攻击的步骤165二、缓冲溢出攻击1681、缓冲溢出的概念1682、缓冲溢出攻击的原理1693、缓冲区溢出的保护方法170三、扫描器1711、什么是扫描器1712、常用的端口扫描技术173四、特洛伊木马1751、特洛伊木马的概念1752、木马的工作原理1763、木马的防范180五、网络监听1801、嗅探器(Sniffer)工作原理1802、防止sniffer1823、检测网络监听的方法183六、拒绝服务攻击1841、什么是拒绝服务的攻击1842、针对网络的拒绝服务攻击1853、DDos攻击的原理187七、IP欺骗1891、IP欺骗原理1892、IP欺骗步骤1913、IP欺骗的防止193八、病毒1931、病毒的定义1932、病毒的特征与种类1943、病毒的防治与检测1964、网络病毒198九、网络应急响应1991、网络安全事件1992、应急准备及处理2003、计算机安全应急响应组2024、CERT/CC的组织架构与运行机制2035、建立统一的信息网络安全保障体系203第十一章 入侵检测206一、什么是入侵检测2061、入侵检测的概念2062、入侵检测系统的分类2083、入侵检测的过程209二、入侵检测技术分析2121、技术分类2122、常用检测方法2153、入侵检测技术发展方向216三、入侵检测系统2181、基于网络的入侵检测系统2182、基于主机的入侵检测系统2203、混合入侵检测系统2224、文件完整性检查系统2225、入侵检测系统的评估223四、IDS的标准化2241、入侵检测工作组(IDWG)2242、通用入侵检测框架(CIDF)225第十二章 IP安全227一、概述2271、结构2272、传送模式与通道模式2283、安全关联SA2294、IPsec安全策略231二、封装安全载荷(ESP)2321、封装安全载荷包格式2322、封装安全协议处理233三、验证头(AH)2351、验证头的包格式2352、验证头协议处理236四、INTERNET密钥交换237第十三章 安全套接层(SSL)协议241一、SSL协议的概述241二、SSL记录协议243三、SSL握手协议244思考题247参考实验251实验一使用网络监听工具251实验二实现加解密程序251实验三实现基于挑战-响应的身份认证252实验四使用防火墙252实验五剖析特洛伊木马255实验六使用PGP实现电子邮件安全255参考文献257



章节摘录

插图：3．验证密钥密钥附着一些检错和纠错位来传输，当密钥在传输中发生错误时，能很容易地被检查出来，并且如果需要，密钥可被重传。

接收端也可以验证接收的密钥是否正确。

发送方用密钥加密一个常量，然后把密文的前2~4字节与密钥一起发送。

在接收端，做同样的工作，如果接收端加密后的常数能与发端常数匹配，则传输无错。

4．更新密钥当密钥需要频繁的改变时，频繁进行新的密钥分发的确是困难的事，一种更容易的解决办法是从旧的密钥中产生新的密钥，有时称为密钥更新。

可以使用单向函数进行更新密钥。

如果双方共享同一密钥，并用同一个单向函数进行操作，就会得到相同的结果。

5．存储密钥密钥可以存储在脑子、磁条卡、智能卡中。

也可以把密钥平分成两部分，一半存入终端一半存入ROM密钥。

还可采用类似于密钥加密密钥的方法对难以记忆的密钥进行加密保存。

## <<计算机系统安全>>

### 编辑推荐

《计算机系统安全》为高等学校本科应用型教材之一。

## <<计算机系统安全>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>