<<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

出版时间：高等教育

作者：曹天杰

页数：308

<<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安全的战略高度，“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．o唱．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。

<<计算机系统安全>>

书籍目录

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人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