<<计算机信息安全技术>>

图书基本信息

书名：<<计算机信息安全技术>>

13位ISBN编号：9787040178180

10位ISBN编号：7040178184

出版时间：2005-9

出版时间：高等教育出版社

作者：步山岳

页数：345

前言

在社会面临严重信息安全问题的环境下，国家和各行业对信息安全人才的需求日臻旺盛，而真正具备渊博知识、丰富实践的信息安全人才却不多，远远不能满足社会需求。
因此，学校对培养信息安全人才具有义不容辞的责任。
1.教材特色正是在社会需求动力的推动下，作者经过3年多时间的精心准备，使得教材具有如下特色：
（1）知识实用、丰富、新颖本教材的编写基于应用型人才培养的需要，以知识实用、丰富、新颖为原则，以通过学习计算机信息安全技术基础理论，使学生初步掌握计算机信息安全实用技能为主导目标，为学生今后进一步学习、研究信息安全技术打下坚实的基础。
教材在有限的篇幅中尽可能蕴涵了更多的信息量，语言尽可能做到文字通顺、语言简练、语义清晰而明确，并在不影响对基础知识理解的前提下，尽可能减少“概念性”和“理论性”知识介绍，增加能解决“实际问题”的内容。
同时，吸取了目前已出版的信息安全技术教材、相关信息安全论文的精髓，充分反映了计算机信息安全领域的前沿技术和成果。
（2）完整的信息安全体系目前计算机信息安全研究的主要方向包括密码学、计算机网络安全、计算机病毒、信息隐藏技术、软件保护技术、数据恢复技术和信息安全管理等方面。
本教材力求融合信息安全研究的基础知识与核心内容，全面反映整个计算机信息安全体系。
虽然教材几乎囊括了信息安全的各个方面，但教材的内容只涉及到计算机信息安全体系最基础、最核心的部分。
而这些“最基础、最核心”的知识又是建立在最实用的基础上，学生不但可以从该教材中全面了解到信息安全概貌，同时又可以迅速掌握信息安全技术的基本技能，为学生今后的工作和研究提供方向性指导。
（3）大量的习题与实验教材提供了大量的习题与实验。
习题与实验的编写是建立在对教材内容理解和巩固的基础上，习题中很少涉及到类似理论性推导或证明性问题。
编写习题与实验的目的就是要巩固学生所学的知识，训练学生解决实际问题的能力，这非常适合定位于培养应用型人才的高等院校。

<<计算机信息安全技术>>

内容概要

本教材主要内容有数据加密标准DES、高级加密标准AES、RSA算法、 NTRU公开密钥体制、信息隐藏技术、数字水印、数字签名、单向散列函数、Kerberos 身份验证、公开密钥基础设施PKI、用户ID与口令机制、生物特征识别技术、计算机病毒与黑客原理和防范、网络攻击与防范、网络欺骗与防范、网络安全服务协议、无线网安全、防火墙技术、入侵检测技术、数字取证技术、操作系统安全机制与配置、系统数据备份、用户数据备份、网络数据备份、数据恢复技术、软件静态分析技术、软件动态分析技术、常用软件保护技术、软件加壳与脱壳等。
教材的每章都配有大量习题和实验。

本书可以作为计算机和通信专业本科或专科的教材。
也可以作为信息安全专业和从事信息安全研究的工程技术人员参考书。

<<计算机信息安全技术>>

书籍目录

章节摘录

插图：计算机内部安全是计算机信息在存储介质上的安全，包括计算机软件保护、软件安全、数据安全等。
计算机内部安全要研究的内容也是非常广泛的，如软件的防盗版，操作系统的安全性问题，磁盘上的数据防破坏、防窃取以及磁盘上的数据恢复与拯救技术等问题。
由于磁盘容量大，存取数据方便，磁盘是目前存放计算机信息最常用的载体。
但由于磁性介质都具有剩磁效应现象，保存在磁性存储介质中的数据可能会使存储介质永久性磁化。
所以保存在磁性存储介质上的信息可能会擦除不尽，永久地保留在磁盘上。
因此对于一些重要的信息，尽管已经使用擦除软件等手段擦除过信息，但如果擦除不彻底就会在磁盘上留下重要信息的痕迹，一旦被别人利用，通过使用高灵敏度磁头和放大器可以将磁盘上的信息还原出来，造成机密信息泄漏。
另外在计算机操作系统中，使用类似格式化命令format，或删除命令del时，仅仅能破坏或删除文件的目录结构和文件指针等信息，磁盘上的原有文件内容仍然原封不动地保留在磁盘中，只要不在磁盘中重新存放数据，使用unformat等方法就可以非常完整地将磁盘上的数据恢复出来。
在Windows操作系统中甚至可以从回收站找回被删除的数据，利用这些就可以窃取重要的机密信息。
计算机的信息安全还可以用信息的完整性、可用性、保密性等属性加以说明。
（1）完整性技术是保护计算机系统内软件和数据不被偶然或人为蓄意地破坏、篡改、伪造等的一种技术手段。
只有经过授权的人才能对信息进行修改，并且能够判断出信息是否已被修改，从而保持信息的整体完整性。
完整性是对信息可靠性和精确性的度量。
（2）可用性技术是在用户授权的条件下，无论什么时候，只要用户需要，信息必须是可用的，是可以访问的，信息系统不能拒绝服务。
（3）保密性技术是防止信息失窃和泄露的技术，信息必须按照信息拥有者的要求保持一定的秘密性。
只有得到拥有者的许可，其他人才能获得该信息。
加密是对存储在各种介质上的信息实施保护的有效和必不可少的技术手段。

编辑推荐

《计算机信息安全技术》是由高等教育出版社出版的。

<<计算机信息安全技术>>

版权说明