

<<信息安全技术导论>>

图书基本信息

书名：<<信息安全技术导论>>

13位ISBN编号：9787121051258

10位ISBN编号：7121051257

出版时间：2007-10

出版时间：电子工业

作者：陈克非

页数：277

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>

<<信息安全技术导论>>

内容概要

《高等学校规划教材：信息安全技术导论》是普通高等教育“十一五”国家级规划教材，是一本简洁而又有一定深度的全面介绍信息安全基本理论、方法、技术和实践的教程。

《高等学校规划教材：信息安全技术导论》按照信息安全领域的热点专题安排章节，共分12章，内容包括：信息安全概论、分组密码技术、公钥密码技术、密钥管理与PKI技术、漏洞扫描技术、入侵检测与防火墙技术、互联网安全协议、无线局域网安全、移动通信安全、信息隐藏与数字水印、智能卡技术和信息安全工程学。

《高等学校规划教材：信息安全技术导论》为任课教师免费提供电子课件，附录A给出了相关实验。

《高等学校规划教材：信息安全技术导论》可作为高校计算机、信息安全、电子信息与通信、信息与计算科学和信息管理等专业高年级本科生和研究生教材，也是相关工程技术人员学习信息安全知识的入门读物。

<<信息安全技术导论>>

书籍目录

第1章 信息安全概论	1.1 信息安全现状	1.2 安全威胁	1.2.1 对密码算法攻击	1.2.2 网络监听攻击
	1.2.3 拒绝服务攻击	1.2.4 对应用协议攻击	1.2.5 对软件弱点攻击	1.2.6 利用系统配置攻击
	1.2.7 网络蠕虫病毒	1.3 安全策略	1.3.1 全局的安全观	1.3.2 信息安全策略
	1.4 安全技术	1.4.1 访问控制技术	1.4.2 防火墙技术	1.4.3 网络入侵检测技术
	1.4.4 漏洞扫描技术	1.4.5 安全审计技术	1.4.6 现代密码技术	1.4.7 安全协议
	1.4.8 公钥基础设施 (PKI)	1.4.9 其他安全技术	1.5 安全标准	1.5.1 国外网络安全标准与政策现状
	1.5.2 国内网络安全标准与政策现状	1.5.3 安全标准应用实例分析	1.6 网络信息安全发展趋势展望	1.6.1 网络信息安全发展趋势
	1.6.2 我国的网络信息安全战略	1.7 进阶阅读	本章参考文献	第2章 分组密码技术
2.1 密码学的历史	2.2 香农安全理论	2.2.1 保密系统模型	2.2.2 信息论基础	2.2.3 理论保密性
2.2.4 实际保密性	2.3 分组密码的基本概念	2.3.1 分组密码	2.3.2 分组密码的研究现状	2.4 分组密码设计原理
2.4.1 设计原理	2.4.2 分组密码的结构	2.4.3 轮函数的结构	2.4.4 密钥扩展算法	2.5 典型的分组密码算法
2.5.1 DES算法	2.5.2 IDEA算法	2.5.3 AES算法	2.6 对分组密码的攻击	2.7 分组密码的工作模式
2.7.1 电子密码本模式ECB	2.7.2 密文块链接模式CBC	2.7.3 密文反馈模式CFB	2.7.4 输出反馈模式OFB	2.8 多重加密
2.9 进阶阅读	习题2	本章参考文献	第3章 公钥密码技术	3.1 公钥密码的概念
3.1.1 问题的引出	3.1.2 公钥密码算法的基本思想	3.2 公钥密码学的理论基础	3.2.1 计算复杂度	3.2.2 P问题和NP完全问题
3.2.3 密码与计算复杂度的关系	3.2.4 单向陷门函数	3.3 公钥密码算法	3.3.1 RSA密码算法	3.3.2 基于离散对数的密码算法
3.3.3 椭圆曲线密码算法	3.4 密钥交换	3.4.1 Diffie-Hellman密钥交换	3.4.2 ECC密钥交换	3.5 公钥密码算法的应用
3.5.1 信息加密	3.5.2 数字签名	3.6 进阶阅读	习题3	本章参考文献
第4章 密钥管理与PKI技术	第5章 漏洞扫描技术	第6章 入侵检测与防火墙技术	第7章 互联网安全协议	第8章 无线局域网安全
第9章 移动通信安全	第10章 信息隐藏与数字水印	第11章 智能卡技术	第12章 信息安全工程学	附录A 信息安全相关实验

<<信息安全技术导论>>

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>