<<信息安全概论>>

图书基本信息

书名：<<信息安全概论>>

13位ISBN编号：9787115159793

10位ISBN编号：7115159793

出版时间：2007-8

出版时间：人民邮电

作者：徐茂智

页数：235

<<信息安全概论>>

内容概要

本书系统介绍信息安全的基本概念、基础理论和前沿技术知识。
全书分为10章，从信息安全基本概念和技术体系出发，先介绍密码保护、身份识别、访问控制为核心的数据安全理论，再围绕网略安全、系统安全、应用安全、安全审计介绍信息安全中涉及的保护、检测和恢复技术，最后介绍信息安全评估与工程实现。
本书注重知识的系统性和覆盖面的宽泛性，而且部分内容有一定深度。
　　本书可以作为信息安全、数字、计算机、微电子专业的研究生和本科生教材，也可以作为相关专业的工程技术人员的参考书。

<<信息安全概论>>

书籍目录

第1章　信息安全简介　1.1　信息安全的发展历史　1.1.1　通信保密科学的诞生　1.1.2　公钥密码学革命　1.1.3　访问控制技术与可信计算机评估准则　1.1.4　网络环境下的信息安全　1.1.5　信息保障　1.2　信息安全的概念和目标　1.2.1　信息安全的定义　1.2.2　信息安全的目标和方法　1.3　安全威胁与技术防护知识体系　1.3.1　计算机系统中的安全威胁　1.3.2　网络系统中的安全威胁　1.3.3　数据的安全威胁　1.3.4　事务安全　1.3.5　技术防护　1.4　信息安全中的非技术因素　1.4.1　人员、组织与管理　1.4.2　法规与道德　小结　习题1第2章　信息安全体系结构　2.1　技术体系结构概述　2.1.1　物理环境安全体系　2.1.2　计算机系统平台安全体系　2.1.3　网络通信平台安全体系　2.1.4　应用平台安全体系　2.2　安全机制　2.2.1　加密　2.2.2　数字签名　2.2.3　访问控制　2.2.4　数据完整性　2.2.5　身份识别　2.2.6　通信量填充与信息隐藏　2.2.7　路由控制　2.2.8　公证　2.2.9　事件检测与安全审計　2.2.10　安全恢复　2.2.11　安全标记　2.2.12　保证　2.3　OSI安全体系结构　2.3.1 OSI的7层网络与TCP/IP模型　2.3.2　OSI的安全服务　2.3.3　OSI安全机制　2.3.4　安全服务与安全机制的关系　2.3.5　层次化结构中服务的配置　2.4　应用体系结构　2.4.1　应用层结构与安全模型　2.4.2　安全交换　2.4.3　安全变换　2.5　组织体系结构与管理体系结构　2.5.1　组织体系结构　2.5.2　管理体系结构　小结　习题第3章　密码基础　3.1　密码学的基本概念　3.1.1　密码编码　3.1.2　密码分析　3.2　对称密码算法　3.2.1　分组密码DES　3.2.2　三重DES　3.2.3　AES　3.2.4　其他分组算法　3.2.5　序列密码算法A5　3.3　公钥密码算法　3.3.1　RSA算法　3.3.2　有限域乘法群密码与椭圆曲线密码　3.4　哈希函数　3.4.1　安全哈希函数的定义　3.4.2　MD与SHA　3.4.3　SHA-1算法描述　3.5　数字签名算法　3.5.1　RSA签名算法　3.5.2　EIGamal签名算法　3.6　密码学的新方向　3.6.1　可证明安全性　3.6.2　基于身份的密码技术　3.6.3　量子密码学　小结　习题3第4章　身份识别与消息鉴别第5章　访问控制理论第6章　网络安全第7章　计算机系统安全第8章　应用安全第9章　安全审计第10章　信息安全评估与工程实现 参考文献

版权说明