

<<信息安全技术基础>>

图书基本信息

书名：<<信息安全技术基础>>

13位ISBN编号：9787508489407

10位ISBN编号：7508489403

出版时间：2011-10

出版时间：中国水利水电

作者：张浩军//杨卫东//谭玉波

页数：181

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>

<<信息安全技术基础>>

内容概要

随着计算机和网络应用的普及，信息安全已经成为关系国家政治稳定、经济发展、军事对抗的重要问题。

本书面向实际应用，全面介绍了信息安全保障体系和防御体系，信息安全基本概念、理论背景，以及各种信息安全技术的实现机理，解读信息安全技术的典型应用，帮助读者树立信息安全工程思想。

全书共分11章，分为四大模块：信息安全工程基本思想、密码学、基于密码技术的安全服务、非密码网络安全防御技术。

本书在编写上强调实用性和系统性，适合大专院校计算机、通信、电子商务等相关专业的信息安全课程使用，也可以作为从事计算机、网络工程项目建设与运行维护的技术人员的参考书。

<<信息安全技术基础>>

书籍目录

前言

第1章 绪论

本章学习目标

- 1.1 信息安全问题及其重要性
- 1.2 信息安全威胁实例
- 1.3 信息安全事件分类
- 1.4 本书内容组织与使用指南

本章小结

习题一

第2章 信息安全保障体系

本章学习目标

- 2.1 信息安全保障体系
 - 2.1.1 信息安全的范畴
 - 2.1.2 信息安全属性
 - 2.1.3 信息安全保障体系结构
- 2.2 信息安全防御模型
- 2.3 风险评估与等级保护
 - 2.3.1 等级保护
 - 2.3.2 风险评估
 - 2.3.3 系统安全测评
 - 2.3.4 信息系统安全建设实施
 - 2.3.5 信息安全原则

本章小结

习题二

第3章 密码技术概述

本章学习目标

- 3.1 密码术及发展
- 3.2 数据保密通信模型
- 3.3 对称密码体制
- 3.4 公钥密码体制
- 3.5 数字签名
- 3.6 消息完整性保护
- 3.7 认证
- 3.8 计算复杂理论
- 3.9 密码分析

本章小结

习题三

第4章 对称密码技术

本章学习目标

- 4.1 数据加密标准DES
 - 4.1.1 概述
 - 4.1.2 DES工作过程
 - 4.1.3 密钥调度
 - 4.1.4 DES安全性分析
 - 4.1.5 3DES

<<信息安全技术基础>>

4.2 高级加密标准AES

4.2.1 AES基本操作流程

4.2.2 轮操作

4.2.3 密钥扩展

4.2.4 解密操作

4.3 其他分组密码算法介绍

4.3.1 IDEA算法

4.3.2 Blowfish算法

4.3.3 RC5 / RC6算法

4.4 流密码算法RC4

4.5 分组密码工作模式

4.5.1 电子密码本

4.5.2 密文分组链接

4.5.3 密文反馈

4.5.4 输出反馈

4.5.5 计数模式

本章小结

习题四

第5章 公钥密码技术

第6章 密钥管理

第7章 安全协议

第8章 无线局域网(WLAN)安全机制

第9章 网络安全技术

第10章 信息隐藏与数字水印技术

第11章 可信计算

参考文献

章节摘录

版权页：插图：对信息系统进行全面的风险评估，这需要对信息系统的应用需求、网络基础设施、外部内部环境、安全威胁、人员、政策法规、安全技术等具有全面的了解，并善于应用各种方法、手段、工具对系统风险进行人工和自动分析，给出全面细致的风险评估。

例如，可以使用自动扫描工具扫描内部网络拓扑，扫描主机、服务器、防火墙、路由器配置，扫描操作系统、数据库、应用系统配置，利用缺陷扫描工具检测系统存在的漏洞或安全弱点等。

从而提出修复、补救、防护建议与措施，并为安全策略制定提供依据。

风险评估要分析出威胁来源与方式，分析系统的脆弱性，评估资产与风险，考虑使用什么强度的保护可以消除、避免、转嫁风险，剩下的风险能否承受。

需要确定用户能够承受的适度风险，从而在这个基础上考虑系统建设，实现投资效益最大化，即安全保障投资与保护资产成正比，而非盲目追求所谓的绝对安全（不存在绝对安全）。

2.制定策略安全策略是安全模型的核心，防护、检测、响应和恢复各个阶段都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。

策略体系的建立包括安全策略的制订、评估、执行等。

制订科学并切实可行的安全策略取决于对网络信息系统的了解程度。

3.实施保护安全保护就是采用一切可能的方法、手段和技术防护信息及信息系统遭受安全威胁，减少和降低遭受入侵和攻击的可能，即实现保密性、完整性、可用性、可控性和不可否认性等安全属性。应该依据不同等级的系统安全要求来完善系统的安全功能、安全机制，如采用加密、认证、防火墙等技术。

<<信息安全技术基础>>

编辑推荐

《信息安全技术基础》突出网络环境下信息安全保障体系的建立和相关技术，面向实用。以网络环境的信息安全保障技术为主线，重点突出以密码技术为基础的安全机制与服务。在编写上强调实用性和系统性，适用于大专院校计算机、通信、电子商务等相关专业的信息安全课程使用。

<<信息安全技术基础>>

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>