

<<无线通信安全理论与技术>>

图书基本信息

书名：<<无线通信安全理论与技术>>

13位ISBN编号：9787563526888

10位ISBN编号：7563526889

出版时间：2011-9

出版时间：北京邮电大学出版社

作者：李晖，牛少彰 编著

页数：358

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>

<<无线通信安全理论与技术>>

内容概要

李晖编著的《无线通信安全理论与技术(普通高校信息安全系列教材)

》主要围绕无线通信安全的主要理论与技术进行研究和讨论。

本书共分4部分,第1部分是入门篇,包括第1,2章,分别介绍无线通信和无线通信安全的历史、分类和基本概念;第2部分是理论篇,由第3~8章组成,介绍无线通信安全的理论基础——密码学的基础知识,包括密码学概述、对称密码体制、公钥密码体制(非对称密码体制)、认证理论基础、数字签名、安全协议等内容;第3部分是实例篇,由第9~17章组成,内容包括gsm, gprs, 窄带cdma, wcdma, tetra等移动通信网络的安全技术,以及wlan, ad

hoc, wimax和蓝牙等无线通信网络的安全技术;第4部分是进展篇,由第18~

21章组成,介绍移动可信计算,移动电子商务安全、传感器网络安全和移动数字版权保护等相关内容

。

《无线通信安全理论与技术(普通高校信息安全系列教材)》适合作为高校信息安全相关专业的本科及研究生教材,也可作为对密码学、信息安全、通信安全等内容感兴趣的技术人员或科研人员的参考读物。

<<无线通信安全理论与技术>>

书籍目录

第1部分 入门篇

第1章 无线通信入门

- 1.1 无线通信的历史
- 1.2 无线通信基本技术
- 1.3 无线通信网络分类
- 1.4 无线通信的研究机构和组织

第2章 无线通信安全入门

- 2.1 无线通信安全历史
- 2.2 无线通信网的主要安全威胁
- 2.3 移动通信系统的安全要求
- 2.4 移动通信系统的安全体系

第2部分 理论篇

第3章 密码学概述

- 3.1 密码学的基本概念
- 3.2 密码体制分类
- 3.3 古典密码简介
- 3.4 密码体制安全性

第4章 对称密码体制

- 4.1 序列密码概述
- 4.2 典型序列密码算法
- 4.3 分组密码理论
- 4.4 典型分组密码算法
- 4.5 密码运行模式

第5章 公钥密码体制

- 5.1 公钥密码的基本概念
- 5.2 rsa密码体制
- 5.3 椭圆曲线密码体制
- 5.4 ntru公钥密码

第6章 认证理论基础

- 6.1 认证的基本概念和认证系统的模型
- 6.2 认证函数
- 6.3 杂凑函数
- 6.4 md4和md5算法
- 6.5 安全杂凑算法(sha)

第7章 数字签名

- 7.1 数字签名基本概念
- 7.2 常用数字签名技术简介
- 7.3 特殊数字签名

第8章 安全协议

- 8.1 安全协议概述
- 8.2 身份认证协议
- 8.3 密钥建立协议

第3部分 实例篇

第9章 gsm系统安全

- 9.1 gsm系统简介

<<无线通信安全理论与技术>>

9.2 gsm系统的安全目标和安全实体

9.3 gsm系统的鉴权机制

9.4 gsm系统的加密机制

9.5 gsm系统的匿名机制

9.6 gsm系统的安全性分析

第10章 gprs安全

10.1 gprs简介

10.2 gprs系统的鉴权

10.3 gprs系统的加密机制

10.4 gprs系统的匿名机制

10.5 安全性分析

第11章 窄带cdma安全

11.1 cdma系统简介

11.2 cdma系统的鉴权

11.3 cdma系统的空口加密

11.4 cdma中的密钥管理

第12章 wcdma安全

12.1 3g系统概述

12.2 3g安全结构

12.3 认证与密钥协商机制

12.4 空中接口安全机制

12.5 核心网安全

12.6 应用层安全

12.7 wpki介绍

第13章 数字集群通信系统安全

13.1 数字集群系统及其标准简介

13.2 tetra标准及网络结构

13.3 tetra系统的基本鉴权过程

13.4 空中接口加密

13.5 tetra系统端到端安全

第14章 无线局域网安全

14.1 无线局域网的结构

14.2 IEEE 802.11 WEP的工作原理

14.3 针对WEP的分析

14.4 IEEE 802.11i的主要加密机制

第15章 wimax安全

15.1 wimax简介

15.2 wimax安全子层

第16章 移动ad hoc网络安全

16.1 移动ad hoc网络简介

16.2 移动ad hoc网络的密钥管理

16.3 移动ad hoc网络的安全路由

第17章 蓝牙安全

17.1 蓝牙技术简介

17.2 蓝牙安全概述

17.3 加密

17.4 认证

<<无线通信安全理论与技术>>

第4部分 进展篇

第18章 移动可信模块

- 18.1 可信计算概念
- 18.2 可信计算平台(tcp)
- 18.3 移动可信模块(mtm)
- 18.4 总结

第19章 基于rfid的移动电子支付安全

- 19.1 概述
- 19.2 rfid技术
- 19.3 rfid安全
- 19.4 基于rfid的移动电子支付安全
- 19.5 总结

第20章 传感器网络安全

- 20.1 无线传感器网络概述
- 20.2 无线传感器网络安全挑战与措施
- 20.3 无线传感器网络的认证机制
- 20.4 无线传感器网络中的加密技术
- 20.5 无线传感器网络的密钥管理
- 20.6 总结

第21章 移动版权保护

- 21.1 数字版权管理系统
- 21.2 omadrm 2.0标准
- 21.3 移动版权保护的发展趋势
- 21.4 总结

参考文献

<<无线通信安全理论与技术>>

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>