

<<通信系统安全>>

图书基本信息

书名：<<通信系统安全>>

13位ISBN编号：9787118083422

10位ISBN编号：7118083429

出版时间：2012-9

出版时间：国防工业出版社

作者：张焕炯

页数：186

字数：275000

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>

<<通信系统安全>>

内容概要

《通信系统安全》(作者张焕炯)以通信系统中的安全问题为研究对象,尝试以信息论等为研究问题的基本工具,对于各种通信模式的安全问题进行了深入的讨论。

全书共分6章:第

1章从信息安全和通信系统的基本概念出发,阐述了通信系统安全这一学科的基本特征和研究方法;第2章从概率论的角度出发,系统地介绍了信息论中的自信息和互信息这两个基本概念,这些概念对于解决通信安全问题有直接的指导作用。

第3章则着重介绍加密算法和认证技术;第4章简要地介绍了各种通信网,并为通信网络中的安全通信问题做了必要的准备;第5章介绍通信网络的安全通信技术;第6章介绍通信系统安全中的非技术因素对安全的影响。

这样建构成一个相对完整的知识体系,把通信系统安全中的最基本的处理问题的理论、方法、技巧等进行较系统的梳理和总结。

《通信系统安全》既可以作为高等院校的教材,也可以作为通信类和信息安全类的相关参考书。

此外,对于想较深入地了解信息理论和网络理论的读者来说,本书也不失为一本能窥探门径的专著。

<<通信系统安全>>

书籍目录

第1章 绪论

- 1.1 信息安全与通信系统
- 1.2 通信系统中的安全问题
- 1.3 通信系统的发展与信息安全理论与实践的关系
- 1.4 通信系统安全的研究方法
- 1.5 小结

思考题

第2章 信息论基础

- 2.1 信息的特征
 - 2.1.1 信息名称的历史沿革
 - 2.1.2 信息量的描述
 - 2.1.3 事件不确定性的概率描述
- 2.2 信息量
 - 2.2.1 自信息量
 - 2.2.2 熵的性质
 - 2.2.3 互信息量
- 2.3 保密通信系统的信息论理论
 - 2.3.1 概述
 - 2.3.2 香农保密定理
 - 2.3.3 唯一解距离与明文规律性函数
 - 2.3.4 分析保密系统的时效性及计算复杂度
- 2.4 小结

思考题

第3章 加密算法与认证技术

- 3.1 加密算法
- 3.2 单钥制密码加密
 - 3.2.1 流密码
 - 3.2.2 块密码
 - 3.2.3 单钥制的密钥分配与管理
- 3.3 公钥制密码加密算法
 - 3.3.1 公钥制密码体制的一般性原理
 - 3.3.2 公钥制密码算法举例
 - 3.3.3 公钥制密钥管理
- 3.4 认证技术
 - 3.4.1 概述
 - 3.4.2 消息认证
 - 3.4.3 数字认证
 - 3.4.4 身份认证
- 3.5 小结

思考题

第4章 通信网技术

- 4.1 通信网络
 - 4.1.1 通信网的基本概念与结构
 - 4.1.2 通信网的分类与发展趋势
- 4.2 典型通信网络分析

<<通信系统安全>>

- 4.2.1 典型有线网络
- 4.2.2 典型无线网络
- 4.2.3 智能网和电信管理网
- 4.3 小结

思考题

第5章 通信网安全通信协议

- 5.1 通信网安全通信协议概述
- 5.2 互联网TCP / IP协议的安全问题
 - 5.2.1 TCP / IP协议族的安全隐患
 - 5.2.2 通信协议族协议受攻击分类
- 5.3 通信网基于TCP / IP协议族的安全通信协议
- 5.4 接入层安全通信协议
 - 5.4.1 点对点隧道协议
 - 5.4.2 第二层隧道协议
- 5.5 网间层安全通信协议
 - 5.5.1 IPsec概述
 - 5.5.2 认证头协议
 - 5.5.3 封装安全载荷协议
 - 5.5.4 Internet密钥交换协议
- 5.6 传送层安全通信协议
 - 5.6.1 安全套接层协议
 - 5.6.2 TLS协议
- 5.7 应用层安全通信协议
 - 5.7.1 概述
 - 5.7.2 电子邮件中的PGP协议
 - 5.7.3 安全超文本传输协议
 - 5.7.4 安全电子交易协议
- 5.8 无线网络的安全通信协议
 - 5.8.1 无线系统的安全性能
 - 5.8.2 无线应用协议的安全性能
 - 5.8.3 有线局域网安全
- 5.9 小结

思考题

第6章 通信系统非技术因素的安全保障

- 6.1 安全保障概述
- 6.2 操作安全
- 6.3 环境因素
- 6.4 道德约束
- 6.5 法律规章
- 6.6 小结

思考题

参考文献

<<通信系统安全>>

编辑推荐

信息安全，顾名思义是关于信息进行安全地传输和存储等处理的理论和技术的总和，在信息化时代，涉及信息安全的领域已不仅仅局限于传统的政治、军事、经济等方面了，它有了非常广泛的拓展，几乎到了无所不包含的程度，在生物信息学、医学信息、图书信息管理、市场、信息经济学理论等方面都离不开信息安全。

《信息安全系列丛书：通信系统安全》以通信系统中的安全问题为研究对象，以信息论和系统论为研究问题的基本工具，对于各种通信模式的安全问题进行了深入的讨论，试图从中寻找到它们内在的共同规律，以期对通信系统理论和通信模式有更深刻的认知，并希望成为通信系统安全这一学科的专著

。

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>