

<<无线网络安全>>

图书基本信息

书名：<<无线网络安全>>

13位ISBN编号：9787120000585

10位ISBN编号：7120000586

出版时间：2004-7

出版时间：电子工业出版社

作者：金纯等编

页数：206

字数：348000

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>

## <<无线网络安全>>

### 内容概要

全书分10章：第1、2章为常用加密和签名算法基础；第3章介绍短距离低功耗无线通讯技术标准，即蓝牙技术的安全性；第4章介绍无线网络以广播方式在物理层传送报文带来的安全威胁和IEEE 802.11认证服务；第5章介绍广泛使用的移动通信系统的安全机制；第6章具体介绍红外光通信系统的安全结构、安全策略和发展趋势；第7章介绍卫星通信网络的组成、安全策略和发展趋势；第8章介绍病毒和攻击等安全威胁及其防护措施及安全策略；第9章从无线网络干扰的角度介绍各种抗自然和人为干扰的技术和发展趋势；第10章介绍目前尚未最后形成业界公认的统一标准的第三代无线通信系统（3G系统）的组成结构，安全网络和安全机制。

本书可供从事无线网络安全设计、系统维护和应用开发的技术人员阅读，也可作为相关专业师生的教学参考书。

## 书籍目录

第1章 加密算法基础及经典加密算法 1.1 加密算法中常用的数论知识 1.1.1 素数和互为素数 1.1.2 模运算 1.1.3 同余类 1.1.4 欧拉定理 1.2 群和有限域 1.2.1 群 1.2.2 域 1.3 加密算法概述 1.3.1 常规密码体制 1.3.2 公钥密码体制 1.4 几种常用经典加密算法介绍 1.4.1 RSA加密算法 1.4.2 椭圆曲线加密算法 (ECC) 1.4.3 数据加密标准 (DES) 1.4.4 RC 1.4.5 安全散列函数MD第2章 数字签名与鉴别协议 2.1 数字签名 2.1.1 数字签名的历史 2.1.2 数字签名的应用需求 2.1.3 直接数字签名 2.1.4 需仲裁的数字签名 2.2 鉴别协议 2.2.1 相互鉴别 2.2.2 单向鉴别 2.3 数字签名标准 2.3.1 DSS方法 2.3.2 数字签名算法 2.3.3 数字签名实现方法 2.3.4 数字证书和互操作标准 2.4 认证中心 (CA) 2.4.1 认证中心 (CA) 简介 2.4.2 CA/RA简介 2.4.3 认证中心的功能 2.4.4 认证中心的主要应用第3章 蓝牙安全性 3.1 蓝牙技术及其安全机制简介 3.2 与蓝牙安全性有关的几个重要参数 3.3 链路字 (密钥) 的分类及其生成算法 3.3.1 链路字的分类 3.3.2 产生链路字的算法 3.4 链路字的生成及传递过程 3.4.1 初始字的生成及传递过程 3.4.2 主单元字的生成及传递过程 3.4.3 单元字的生成及传递过程 3.4.4 组合字的生成及传递过程 3.5 鉴权 (Authentication) 3.6 加密 (Encryption) 3.7 有关蓝牙安全算法的几个函数 3.7.1 鉴权函数E 3.7.2 链路字生成函数E 3.7.3 Kc的生成函数E 3.7.4 加密算法E 3.8 蓝牙安全性存在问题的讨论 3.8.1 初始字 3.8.2 单元字 3.8.3 鉴权过程 3.8.4 蓝牙设备地址 3.9 总结第4章 IEEE 802.11的安全性 4.1 有关IEEE 802.11家族安全性的理论知识 4.1.1 两类认证服务 4.1.2 有线等同加密 (WEP) 算法 4.2 IEEE 802.11安全性在实践中的应用 4.2.1 IEEE 802.11的保密机制 4.2.2 IEEE 802.11b安全机制的缺点 4.2.3 解决方案第5章 移动通信系统的安全 5.1 移动通信系统概述 5.1.1 GSM移动通信系统 5.1.2 CDMA移动通信系统 5.1.3 GPRS和CDMA 1X系统 5.1.4 WCDMA、CDMA2000和TD-SCDMA系统 5.1.5 未来的移动通信系统 5.2 GSM的安全策略 5.2.1 鉴权中心和SIM卡 5.2.2 鉴权 5.2.3 加密 5.2.4 用户身份保护 5.2.5 安全性分析 5.3 GPRS的安全策略 5.3.1 鉴权 5.3.2 数据加密 5.3.3 安全性分析 5.4 CDMA的安全策略 5.4.1 移动识别参数 5.4.2 鉴权 5.4.3 SSD的更新 5.4.4 加密 5.5 第三代移动通信系统 (3G) 的安全策略 5.5.1 2G的安全缺陷 5.5.2 3G的安全结构 5.5.3 3G的安全特性 5.6 移动多跳分组无线网络 (Ad Hoc) 的安全性 5.6.1 Ad Hoc网络及其面临的安全威胁 5.6.2 Ad Hoc网络的安全技术 5.6.3 Ad Hoc网络的入侵检测 5.6.4 小结参考文献第6章 红外光通信的安全 6.1 概述 6.2 红外光通信的网络结构 6.3 红外光通信的安全性 6.3.1 背景噪声 6.3.2 信号的损耗与衰落 6.3.3 其他安全威胁 6.4 总结参考文献第7章 卫星通信的安全问题 7.1 卫星通信系统概述 7.1.1 卫星通信系统的组成 7.1.2 卫星通信系统的分类 7.2 卫星通信系统的网络物理安全 7.2.1 网络可靠性 7.2.2 网络控制 7.3 卫星通信系统的保密技术 7.3.1 数据加密方案 7.3.2 密钥的分发与管理 7.3.3 身份认证 7.3.4 其他安全措施 7.4 总结参考文献第8章 无线网络的安全 8.1 无线网络的安全结构 8.1.1 无线网络的传输方式 8.1.2 无线网络的一般结构 8.1.3 无线网络的安全缺陷 8.1.4 无线网络的安全策略 8.2 无线病毒 8.2.1 病毒的基本特征及其分类 8.2.2 无线病毒的主要传播途径 8.2.3 无线病毒的防范措施 8.2.4 反无线病毒产品 8.3 手机病毒 8.3.1 手机病毒的攻击原理 8.3.2 黑客对手机攻击的方式 8.3.3 手机病毒的防治 8.4 黑客对无线网络的威胁 8.4.1 黑客网络攻击的一般过程和主要类型 8.4.2 无线网络反黑客对策 8.5 战术网络安全 8.5.1 数字化战场与战斗信息网WIN 8.5.2 战斗信息网WIN的安全风险分析 8.5.3 战斗信息网WIN的安全 8.5.4 战斗信息网WIN中的安全设置 8.6 总结参考文献第9章 无线通信的抗干扰 9.1 无线通信面临的干扰威胁 9.1.1 传播环境对无线通信的影响 9.1.2 无线通信系统自身的干扰 9.1.3 无线通信干扰技术 9.2 抗干扰技术及其发展趋势 9.2.1 功率控制技术 9.2.2 扩频通信技术 9.2.3 纠错编码技术 9.2.4 自适应天线技术 9.3 总结参考文献第10章 第三代移动通信系统安全特点介绍 10.1 概述 10.1.1 第三代移动通信系统 (3G) 的安全规则 10.1.2 第二代移动通信系统安全方面的弱点 10.1.3 3G保留2G系统以及进一步开发的安全特点 10.1.4 第三代移动通信系统新的安全和服务特性 10.1.5 第三代移动通信系统的安全目标 10.2 第三代移动通信系统的安全威胁 10.2.1 第三代移动通信系统的数据类型 10.2.2 第三代移动通信系统的安全威胁 10.2.3 第三代移动通信系统的安全要求 10.3 第三代移动通信系统的安全体系结构概述 10.4 第三代移动通信系统的安全特性 10.4.1 网络访问安全 10.4.2 安全的能见度和可配置性 10.5 第三代移动通信系统的网络访问安全机制 10.5.1 通过临时身份进行识别 10.5.2 通过永久身份进行识别

10.5.3 鉴权和密钥协议 10.5.4 本地鉴权和本地连接建立 10.5.5 访问链数据完整性 10.5.6 访问链数据机密性附录A 本章所用符号附录B 缩写词列表参考书目

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>