<<无线局域网安全系统>>

图书基本信息

书名：<<无线局域网安全系统>>

13位ISBN编号：9787505396579

10位ISBN编号：7505396579

出版时间：2004-3

出版时间：电子工业出版社

作者：曹秀英

页数：211

字数：360000

<<无线局域网安全系统>>

内容概要

本书针对IEEE 802.11系列标准，对无线局域网安全系统进行研究。
全书共分上、中、下三篇，主要讲述了无线局域网安全系统的基本理论和实际应用，其中包括无线局域网标准概述、IEEE 802.11标准、无线局域网密钥管理协议、RADIUS协议、RC4算法、TKIP密码协议、AES算法分析、WRAP与CCMP密码协议、ECC体制、安全无线局域网的实现方案、无线局域网AP和网卡的嵌入式硬件设计、IEEE 802.11 MAC层的软件实现、无线局域网安全认证和密钥管理系统的实现、RADIUS服务器在WLAN中的实现等方面内容。

本书可作为网络通信领域的工程技术人员和科研人员的参考书，也可供高等院校通信与信息系统专业的本科生、研究生阅读。

作者简介

曹秀英：女，教授，东南大学移动通信国家重点实验室副主任，主要研究方向为无线通信与信息安全技术。
作为项目负责人主持了多项国家级和省部级项目的研究，具有代表性的项目有“新一代模数模全双工保密机研究”、“模拟保密机应用基础研究”、“虑拟专用网络关键技术研究

<<无线局域网安全系统>>

书籍目录

上篇 概述 第1章 绪论（3） 1.1 无线局域网标准概述（3） 1.2 IEEE 802.11标准简介（4） 1.3 无线局域网安全系统（5） 1.4 无线局域网的优点及应用（5） 1.5 未来的无线局域网（6） 第2章 IEEE 802.11标准（9） 2.1 IEEE 802.11 标准体系结构（9） 2.2 IEEE 802.11 MAC层协议（9） 2.2.1 IEEE 802.11 MAC协议概述（10） 2.2.2 分布式网络访问控制方式（DCF）（11） 2.2.3 中心网络访问控制方式（PCF）（14） 2.2.4 MAC帧格式（15） 2.2.5 MAC层DCF的仿真（17） 2.3 IEEE 802.11 物理层（22） 2.4 本章小结（24） 参考文献（24）中篇 基本理论与分析 第3章 网络安全的基本概念（27） 3.1 网络面临的安全威胁（27） 3.2 网络安全业务（28） 3.3 IEEE 802.11标准安全部分概述（29） 3.4 本章小结（29） 参考文献（30） 第4章 IEEE 802.11中的安全技术（31） 4.1 IEEE 802.11安全技术概述（31） 4.1.1 无线局域网网络结构（31） 4.1.2 无线局域网系统的业务（32） 4.1.3 无线局域网安全业务（32） 4.2 IEEE 802.11的安全漏洞分析（35） 4.3 IEEE 802.11的安全解决方案（37） 4.4 本章小结（38） 参考文献（38） 第5章 IEEE 802.1X认证协议（40） 5.1 IEEE 802.1X提出背景（40） 5.2 IEEE 802.1X的体系结构（40） 5.3 端口控制原理（41） 5.3.1 逻辑端口的概念（41） 5.3.2 端口控制原理（42） 5.4 IEEE 802.1X的认证过程（42） 5.5 可扩展认证协议——EAP协议（43） 5.5.1 EAP可扩展认证协议（43） 5.5.2 EAP协议在IEEE 802.1x中的应用（44） 5.6 IEEE 802.1X协议的其他内容（47） 5.7 协议实现的状态机（47） 5.7.1 Supplicant状态机（47） 5.7.2 Authenticator的状态机（48） 5.7.3 后端服务器的状态机（49） 5.8 IEEE 802.1X协议的优点（50） 5.9 TLS协议（51） 5.9.1 EAP支持的认证协议（51） 5.9.2 TLS传输层安全协议（51） 5.9.3 TLS协议的安全性（55） 5.9.4 EAP-TLS数据包格式（55） 5.9.5 EAP-TLS认证过程（56） 5.10 本章小结（58） 参考文献（58） 第6章 无线局域网密钥管理协议（59） 6.1 密钥管理的基本概念（59） 6.1.1 密钥管理的目的（59） 6.1.2 密钥的种类（59） 6.2 无线局域网的密钥管理系统（59） 6.2.1 强安全网络RSN的安全性能协商（60） 6.2.2 认证和密钥管理系统（60） 6.2.3 密钥层次（61） 6.3 四步握手密钥协商机制（63） 6.3.1 四步握手密钥初始化（63） 6.3.2 四步握手过程（64） 6.3.3 组密钥更新（65） 6.4 四步握手机制的状态机（66） 6.4.1 申请者状态机（66） 6.4.2 认证者状态机（66） 6.5 EAPOL-KEY消息的封装（67） 6.6 IEEE 802.1X密钥管理协议的优点（70） 6.7 本章小结（70） 参考文献（70） 第7章 RADIUS协议（71） 7.1 AAA概述（71） 7.2 RADIUS协议（71） 7.3 RADIUS的EAP扩展协议（78） 7.4 RADIUS计费协议（80） 7.5 RADIUS协议的安全性（82） 7.6 本章小结（83） 参考文献（83） 第8章 RC4算法（85） 8.1 RC4算法简介（85） 8.2 RC4算法的一般分析（85） 8.3 RC4算法的INVARIANCE WEAKNESS攻击（86） 8.4 RC4算法的IV WEAKNESS攻击（87） 8.5 WEP2密码协议（91） 8.6 变形算法RC4*（91） 8.7 本章小结（92） 参考文献（92） 第9章 TKIP密码协议（93） 第10章 AES算法分析（105） 第11章 WRAP与CCMP密码协议（117） 第12章 椭圆曲线密码体制（ECC）（135）下篇 实际应用 第13章 安全无线局域网的实现方案（155） 第14章 无线局域网AP和网卡的嵌入式硬件设计（164） 第15章 IEEE 802.11 MAC层的软件实现（180） 第16章 无线局域网安全认证和密钥管理系统的实现（191） 第17章 RADIUS服务器在WLAN中的实现（201）后记（211）

<<无线局域网安全系统>>

版权说明