

<<IPSec解析>>

图书基本信息

书名：<<IPSec解析>>

13位ISBN编号：9787118044133

10位ISBN编号：711804413X

出版时间：2006-5

出版时间：国防工业出版社

作者：周贤伟

页数：191

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>

<<IPSec解析>>

内容概要

本书从实用和科研的角度出发, 比较全面、系统地介绍了IPsec及相关安全技术的最新发展。

全书共分14章, 系统、全面地介绍了IPsec技术, 详细分析了密码技术、TCP/IP技术、IPsec体系结构和组件、身份认证和保密性机制、认证头和封装安全载荷的用法以及密钥交换、IP压缩、IPsec实施等技术。

本书内容翔实, 深入浅出, 覆盖面广, 具有先进性、科学性和很高的实用价值, 适合于高等院校计算机、通信、信息安全等专业师生以及对IPsec感兴趣的科研人员和工程技术人员选做参考用书。

作者简介

周贤伟，四川成都人，博士后，1986年毕业于西南师范大学获学士学位，1992年毕业于郑州大学获硕士学位，1999年毕业于西南交通大学获博士学位，2001年出站于北京交通大学信息与通信工程学科博士后流动站。

国家科技部条件平台建设通信技术项目评审专家组成员，国家自然科学基金通信学科评审专家，《电波科学学报》编委。

在《电子学报》等重要刊物发表学术论文50多篇，其中多篇被SCI和EI收录。

主持并承担国家“863”重大项目1项，国家自然科学基金项目1项，军队预研项目6项，博士后科研基金2项，国家中小企业创新基金以及企业项目多项；申请国家发明专利3项；译著《OpenCable体系结构》1部。

目前感兴趣的研究方向主要有移动通信、下一代网络、电波传播技术和信息安全等。

<<IPSec解析>>

书籍目录

第1章 密码学概述1.1 网络安全1.2 加密方法1.2.1 加密基础1.2.2 公钥密码体制1.2.3 常用公钥加密算法1.2.4 对称密码技术1.2.5 对称密钥密码学与公钥密码学的比较1.2.6 量子密码1.2.7 密钥交换1.2.8 数字签名1.3 安全性评估模型参考文献第2章 公钥基础设施2.1 PKI简介2.2 数字证书2.3 PKI的信任模型2.3.1 PKI单级模型2.3.2 分级信任模型2.3.3 PKI与IPSec2.4.PKI 在信息安全中的应用2.4.1 安全电子邮件2.4.2 Web安全2.4.3 电子商务的应用参考文献第3章 TCP/IP综述3.1 TCP/IP的历史3.2 TCP/IP协议的体系结构3.2.1 TCP/IP的层次3.2.2 数据流3.3 网际协议IP3.3.2 IPv63.3.3 分段3.3.4 ICMP3.3.5 IP组播3.4 移动IP3.4.1 移动IPv4的功能实体3.4.2 移动IPv4的其他常见术语3.4.3 移动IPv4的基本操作3.4.4 移动IPv6和移动IPv4的比较3.5 传输层3.6 实施保密的层次3.6.1 应用层安全3.6.2 传输层安全3.6.3 数据链路层安全3.6.4 网络层安全参考文献第4章 IP安全综述4.1 IP安全需求4.1.1 网络安全概述4.1.2 Internet攻击类型4.1.3 IPSec的引入4.2 IPSeec体系结构4.3 认证头4.4 封装安全载荷4.5 Internet密钥交换4.5.1 Internet简单密钥管理协议的发展历程4.5.2 相关概念4.5.3 IKE的两阶段协商4.5.4 IKE交换过程4.5.5 IKE的安全性4.6 移动TP中的IPSec4.6.1 移动IP的安全性问题4.6.2 IPSec应用于移动IP4.7 IP 组播安全简介4.7.1 组播通信面临的安全风险4.7.2 组播中的安全问题4.7.3 安全组播与IPSec的兼容性讨论参考文献第5章 IPSec体系结构第6章 认证头第7章 封装安全载荷第8章 Internet密钥交换第9章 策略第10章 IPSec的实施第11章 实用IP安全技术第12章 IP压缩第13章 密钥恢复第14章 IPSec实施案例

<<IPSec解析>>

编辑推荐

本书从实用和科研的角度出发，比较全面、系统地介绍了IPsec及相关安全技术的最新发展。

本书内容翔实，深入浅出，覆盖面广，具有先进性、科学性和很高的实用价值，适合于高等院校计算机、通信、信息安全等专业师生以及对IPsec感兴趣的科研人员和工程技术人员选做参考用书。

<<IPSec解析>>

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>