<<网络安全控制机制>>

图书基本信息

书名：<<网络安全控制机制>>

13位ISBN编号：9787302186731

10位ISBN编号：7302186731

出版时间：2008-12

出版时间：清华大学出版社

作者：林闯，蒋屹新，尹浩　著

页数：309

前言

背景随着传感器、嵌入式设备、消费电子等设施的大量接入，互联网络在规模和应用领域上日益得到拓展，网络的规模仍在继续扩大，网络在国民经济生活中的基础性和全局性作用日益增强。
尽管互联网已经转变并大大改善了人类社会的经济和生活方式，但同时也不得不面临大量的网络安全问题，如恶意攻击、垃圾邮件、计算机病毒、不健康资讯等。
尽管信息网络的安全研究已经持续多年，但对网络攻击和破坏行为的对抗效果并不理想，仍然面临着严峻的挑战。

<<网络安全控制机制>>

内容概要

网络安全是计算机和通信领域很重要的研究方向，而网络安全控制机制是网络安全的基本保障，是网络安全中的重要研究内容。
本书分为5章，第1章是访问控制机制，讲述了访问控制的最新进展，并讨论了移动通信和可信网络环境下的访问控制技术。
第2章是认证机制，介绍AAA服务器的认证原理及其在无线网络中的应用，然后介绍多级安全域的认证模型，最后讨论了移动网络中的可以容忍DoS攻击的认证模型。
第3章是数字签名机制，介绍数字签名中的公钥密码体制和椭圆曲线密码体制，并讨论了基于椭圆曲线的群体导向的签名方案。
第4章是密钥管理机制，概述了基本的组密钥分发机制，讨论了自愈的组密钥分发协议和基于时限的组密钥分发机制，并阐述了无线传感器网络中的密钥管理。
第5章是基于应用层组播的视频安全机制，介绍流媒体与应用层组播，数字水印技术以及视频加密技术，并详细描述了一个视频安全组播协议，讨论了视频流传输过程中的差错控制。
　本书全面、系统地展示了网络安全控制机制的研究内容和最新成果，具有完整性、实用性和学术性。
非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。
既可以供计算机、通信、电子、信息等相关专业的研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

<<网络安全控制机制>>

书籍目录

第1章 访问控制 1.1 访问控制概述 1.1.1 访问控制基本概念 1.1.2 访问控制目标 1.1.3 访问控制发展过程 1.1.4 访问控制分类 1.1.5 访问控制研究趋势 1.2 基于着色Petri网的强制访问控制模型 1.2.1 强制访问控制模型的形式化描述与安全分析 1.2.2 着色Petri网 1.2.3 基于着色Petri网的强制访问控制模型 1.2.4 安全性分析 1.3 支持移动通信的访问控制 1.3.1 移动IPv6 1.3.2 支持移动网络的访问控制 1.3.3 支持层次移动IPv6的访问控制 1.3.4 方案的扩展与分析 1.4 可信网络访问控制与可信网络连接 1.4.1 可信网络 1.4.2 可信网络访问控制 1.4.3 可信计算 1.4.4 可信网络连接 参考文献第2章 认证 2.1 RADIUS协议 2.1.1 RADIUS协议简介 2.1.2 RADIUS的安全处理 2.1.3 RADIUS的工作过程 2.2 AAA服务器设计 2.2.1 AAA系统概述 2.2.2 AAA系统的设计需求 2.2.3 AAA系统的整体结构 2.2.4 AAA系统的基本设计思想 2.2.5 AAA数据流控制设计 2.2.6 RADIUS认证服务器 2.2.7 RADIUS计费服务器 2.2.8 系统冗余容错处理 2.3 下一代AAA协议--Diameter协议 2.3.1 Diameter协议概述 2.3.2 Diameter协议格式 2.3.3 Diameter与RADIUS的比较 2.4 AAA在无线网络中的应用 2.4.1 基本模型 2.4.2 AAA协议漫游的需求 2.4.3 移动IP的AAA 2.4.4 3G-WLAN互联中的AAA 2.5 多级安全域的认证模型 2.5.1 多级安全域的格模型 2.5.2 多级安全域之间的关系 2.5.3 多级安全域认证体系结构 2.5.4 多级安全域的认证协议 2.5.5 利用逻辑理论对安全域认证协议的形式化描述 参考文献第3章 数字签名 3.1 公钥密码体制 3.1.1 密码体制分类 3.1.2 公钥密码体制原理 3.1.3 Diffie-Hellman密钥交换 3.1.4 RSA密码体制 3.1.5 ElGamal密码体制 3.2 数字签名 3.2.1 数字签名基本概念 3.2.2 数字签名的特点 3.2.3 RSA数字签名体制 3.2.4 ElGamal数字签名体制 3.2.5 Schnorr数字签名体制 3.2.6 DSS数字签名体制 3.2.7 几个特殊的数字签名 3.3 椭圆曲线密码体制 3.3.1 椭圆曲线基本概念 ……第4章 密钥管理第5章 基于应用层组播的视频安全英汉对照术语表

章节摘录

插图：

编辑推荐

《网络安全控制机制》由清华大学出版社出版。

<<网络安全控制机制>>