

<<网络安全理论与技术>>

图书基本信息

书名：<<网络安全理论与技术>>

13位ISBN编号：9787115115577

10位ISBN编号：7115115575

出版时间：2003-10

出版时间：人民邮电出版社

作者：杨义先

页数：587

字数：922000

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>

<<网络安全理论与技术>>

内容概要

本书从理论和技术两个方面对网络信息安全的相关知识进行全面和系统介绍。

本书是作者及北京邮电大学信息安全中心近十年来的科研成果的总结，书中大部分内容在国内外同类书籍中较为少见，不少还是首次出现，其体系架构、描述方式和材料取舍都充分考虑了我国现阶段信息化进程的特色。

全书共分四篇，分别介绍网络安全概论、安全网管、安全支付和安全通信。

全书内容覆盖了信息安全保障体系、操作系统与安全、网络系统与安全、数据库系统与安全、防火墙、入侵检测、安全协议、安全网管、电子支付、电子现金、安全微支付、网络银行、安全固网电信系统、安全移动通信系统、安全短信系统、安全邮件系统等网络信息安全理论与技术方面的主要内容。

本书可作为高等学校信息安全、密码学、信息与计算科学、通信与信息系统、信号与信息处理、应用数学、控制理论与控制技术、模式识别与智能系统、计算机系统结构、计算机软件与理论、计算机应用技术、军事通信学、软件工程等专业的研究生和高年级学生的教学参考书，也可作为相关领域科技工作者的实用工具书或技术培训教材。

另外，书中介绍的许多算法、协议、方案等都可以直接应用于工程实践，书中提出的许多理论问题也有助于激发更多的后继研究。

<<网络安全理论与技术>>

书籍目录

- 第一篇 网络安全概论第1章 信息安全保障体系 31.1 深层防御 31.1.1 健全法制 31.1.2 加强管理 51.1.3 完善技术 91.1.4 培养人才 151.2 全面保障 161.2.1 PDRR模型 161.2.2 基础设施 191.2.3 计算环境 231.2.4 区域边界 261.3 安全工程 341.3.1 发掘需求 351.3.2 构建系统 361.3.3 检测评估 381.3.4 风险管理 391.4 技术对策 401.4.1 知己知彼 401.4.2 安全服务 421.4.3 弹性策略 451.4.4 互动策略 47第2章 操作系统与安全 482.1 UNIX与安全 492.1.1 系统用户命令的安全问题 492.1.2 系统用户安全要点 522.1.3 系统管理员命令的安全问题 532.1.4 系统管理员安全要点 562.2 X Window与安全 582.2.1 为什么会出现X Window安全问题 582.2.2 X Window系统实用工具与安全问题 602.2.3 如何提高X Window的安全性 622.2.4 X系统的几个容易被忽略的漏洞 642.3 Windows NT与安全 652.3.1 Windows NT安全简介 652.3.2 Windows NT环境的设置 672.3.3 Windows NT的安全模型 702.3.4 Windows 95/98的安全性 722.4 Linux与安全 722.4.1 Linux体系结构 722.4.2 Linux网络接口 732.4.3 Linux的安全问题 772.4.4 基于Linux的IPSec模型 78第3章 网络系统与安全 813.1 计算机网络基础 813.1.1 计算机网络的过去 813.1.2 计算机网络的现在 823.1.3 计算机网络的分类 853.1.4 计算机网络存取控制方法 883.2 开放系统的参考模型及其安全体系结构 893.2.1 开放系统互连及参考模型 903.2.2 开放系统参考模型分层的原则和优点 913.2.3 ISO/OSI对安全性的一般描述 923.2.4 Novell NetWare结构组成和安全体系结构 933.3 网络中常见的攻击手段 943.3.1 信息收集 953.3.2 口令攻击 963.3.3 攻击路由器 963.3.4 攻击TCP/IP 973.3.5 利用系统接收IP数据包的漏洞 983.3.6 电子邮件攻击 993.3.7 拒绝服务攻击 993.4 常用网络服务的安全问题 1013.4.1 FTP文件传输的安全问题 1013.4.2 Telnet的安全问题 1013.4.3 WWW服务的安全问题 1013.4.4 电子邮件的安全问题 1023.4.5 Usenet新闻的安全问题 1023.4.6 DNS服务的安全问题 1023.4.7 网络管理服务的安全问题 1023.4.8 网络文件系统的安全问题 103第4章 数据库系统与安全 1044.1 数据库系统基础 1044.1.1 数据库系统概念 1044.1.2 管理信息系统 1054.1.3 关系数据库 1094.1.4 数据库管理系统的体系结构 1124.2 数据库系统的安全 1164.2.1 数据库的安全策略 1164.2.2 数据库加密 1174.2.3 数据库的安全性要求 1214.2.4 安全数据库的设计原则 1234.3 Web数据库的安全 1244.3.1 Web与HTTP协议的安全 1244.3.2 CGI程序的安全 1264.3.3 Java与JavaScript的安全 1284.3.4 ActiveX的安全 1294.3.5 Cookie的安全 1304.4 Oracle数据库的安全 1314.4.1 Oracle数据库安全功能概述 1314.4.2 Oracle数据库的安全管理方法 1314.4.3 Oracle数据库的并发控制 134第二篇 安全网管第5章 防火墙 1395.1 防火墙技术概论 1395.1.1 防火墙的优缺点 1395.1.2 防火墙的包过滤技术 1415.1.3 防火墙的应用层网络技术(代理技术) 1465.1.4 防火墙的电路级网关技术 1485.1.5 防火墙的状态检查技术 1505.1.6 防火墙的地址翻译技术 1505.1.7 防火墙的其他相关技术 1515.2 防火墙的体系结构 1525.2.1 包过滤型防火墙 1525.2.2 双宿主机型防火墙 1545.2.3 屏蔽主机型防火墙 1555.2.4 屏蔽子网型防火墙 1565.2.5 其他防火墙体系结构 1575.3 防火墙过滤规则的优化 1575.3.1 基于统计分析的动态过滤规则优化 1575.3.2 基于统计分析的自适应动态过滤规则优化 1605.3.3 基于统计分析的动态过滤规则分段优化 1615.3.4 具有安全检查特性的基于统计分析的动态过滤规则优化 1625.3.5 防火墙过滤规则动态优化的性能分析与仿真 1655.4 基于操作系统内核的包过滤防火墙系统的设计与实现 1685.4.1 预备知识 1685.4.2 基于Windows 9x的NDIS内核模式驱动程序的实现 1705.4.3 基于Windows NT的NDIS内核模式驱动程序的实现 1715.5 PC防火墙的研究与实现 1735.5.1 问题的提出 1735.5.2 PC的安全问题 1735.5.3 PC防火墙及其功能需求 1745.5.4 PC防火墙的一种实现方案 175第6章 入侵检测 1826.1 基础知识 1826.1.1 历史沿革与基本概念 1826.1.2 入侵检测系统的体系结构 1856.1.3 基于知识和行为的入侵检测 1896.1.4 入侵检测系统的信息源 1936.2 入侵检测标准 1976.2.1 入侵检测数据交换标准化 1976.2.2 通用入侵检测框架 1996.2.3 入侵检测数据交换格式 2046.2.4 通用入侵检测框架的语言 2066.3 入侵检测系统模型 2096.3.1 基于系统行为分类的检测模型 2096.3.2 面向数据处理的检测模型 2116.3.3 入侵检测系统和算法的性能分析 2126.3.4 入侵检测系统的机制协作 2146.4 基于进程行为的入侵检测 2176.4.1 基于神经网络的行为分类器

2186.4.2 基于概率统计的贝叶斯分类器 2206.4.3 基于进程行为分类器的入侵检测 2226.4.4 基于进程检测器的入侵检测系统原型 225第7章 安全协议 2267.1 IPsec协议 2267.1.1 IPsec体系结构 2277.1.2 IPsec的实现途径 2367.1.3 IPsec安全性分析 2387.1.4 一种新的分层IPsec体系结构 2457.2 密钥交换协议 2557.2.1 ISAKMP的消息构建方式 2557.2.2 ISAKMP的载荷类型 2567.2.3 安全联盟的协商 2567.2.4 建立ISAKMP SA 2577.2.5 IKE的消息交换流程 2597.3 多方安全协议 2637.3.1 (t,n)门限方案 2637.3.2 Pinch在线机密分享方案及其弱点分析 2647.3.3 单一信息广播的安全协议 2687.3.4 多个信息广播的安全协议 2697.4 公平电子合同 2707.4.1 背景知识 2707.4.2 两方公平电子合同 2717.4.3 多方公平电子合同 274第8章 安全网管 2788.1 安全网管系统架构 2788.1.1 多层次安全防护 2788.1.2 安全网管系统 2798.1.3 系统部署 2808.1.4 功能特点 2818.2 网络控制代理 2818.2.1 网络控制代理的总体设计 2818.2.2 netfilter架构 2828.2.3 攻击防范 2848.2.4 功能模块 2858.3 网络检测代理 2868.3.1 网络检测代理的总体设计 2868.3.2 网络数据的收集 2878.3.3 检测的方法、机制、策略和流程 2888.3.4 功能模块 2918.4 主机安全代理 2928.4.1 主机安全代理的总体设计 2928.4.2 虚拟设备驱动程序技术 2948.4.3 主要功能的实现 2958.4.4 功能模块 2978.5 管理中心 2998.5.1 功能和需求分析 2998.5.2 模块组成 2998.6 系统自身安全 3018.6.1 对付攻击 3018.6.2 安全通信 3028.6.3 设计原则 3058.6.4 应用示例 306第三篇 安全支付第9章 电子支付 3119.1 安全电子交易 3119.1.1 电子支付系统模型 3119.1.2 数字货币 3169.1.3 电子支付系统(EPS) 3179.1.4 电子数据交换 3189.1.5 通用电子支付系统(UEPS) 3199.2 无匿名性的电子支付系统 3209.2.1 First Virtual 3209.2.2 O-card 3229.2.3 iKP 3239.2.4 SET 3249.3 无条件匿名性的电子支付系统 3289.3.1 匿名需求 3289.3.2 盲签名技术 3299.3.3 Ecash 3339.3.4 Brands 3349.4 匿名性受控的电子支付系统 3369.4.1 公平盲签名 3379.4.2 公平的离线电子现金系统 3389.4.3 一种在线的公平支付系统 3409.4.4 基于可信方标记的电子现金系统 3429.4.5 NetCash 343第10章 电子现金 34510.1 基础知识 34510.1.1 历史与现状 34510.1.2 电子现金的基本流程 34910.1.3 电子现金的特点 35010.1.4 电子现金关键技术 35010.2 基于零知识证明的电子现金模型 35010.2.1 基本概念及协议 35110.2.2 零知识证明简介 35310.2.3 基于零知识证明的电子现金模型 35410.2.4 基于RSA盲签名与二次剩余的电子现金方案 35810.3 比特承诺及其应用 36110.3.1 高效比特承诺方案 36210.3.2 基于比特承诺的身份认证方案 36510.3.3 基于比特承诺的部分盲签名方案 36710.3.4 基于部分盲签名的电子现金 37110.4 高效电子现金方案设计 37510.4.1 高效可分电子现金方案 37510.4.2 单项可分电子现金方案 381第11章 安全微支付 38611.1 微支付机制 38611.1.1 基于公钥机制的微支付系统 38711.1.2 基于宏支付的微支付系统 38811.1.3 基于共享密钥机制的微支付系统 38911.1.4 基于散列链的微支付系统 39211.1.5 基于概率机制的微支付系统 39511.1.6 基于散列冲突的微支付系统 39711.2 基于散列链的微支付系统 39811.2.1 基于PayWord的WWW微支付模型 39811.2.2 基于散列链的防欺诈微支付系统 40211.3 分布式环境中的微支付系统 40611.3.1 分布式微支付协议 40611.3.2 基于微支付的反垃圾邮件机制 40911.4 微支付在无线环境中的应用 41511.4.1 移动增值服务支付 41511.4.2 微支付在移动增值服务认证和支付中的应用 41611.4.3 微支付在移动IP认证和支付中的应用 418第12章 网络银行 42512.1 网络银行概述 42512.1.1 网络银行的发展 42512.1.2 网络银行的实现方式 42612.1.3 网络银行的安全性需求 42912.1.4 网络银行的结构与功能 43012.2 基于电子支票的网络银行 43112.2.1 基于对称密码体制的电子支票 43112.2.2 CNOS多签名体制 43412.2.3 基于CNOS多签名的电子支票 43812.3 基于电子现金的网络银行 44112.3.1 性能要求 44112.3.2 不可追踪性与盲签名 44212.3.3 基于OSS的盲签名体制 44512.4 网络银行实例 44812.4.1 网络银行软件结构 44812.4.2 网络银行安全机制 45012.4.3 安全网络证券交易系统 453第四篇 安全通信第13章 安全固定网电信系统 45913.1 电话防火墙 46013.1.1 单机电话防火墙概述 46013.1.2 单机电话防火墙的关键技术 46113.1.3 小型交换机防火墙 46313.2 联机防火墙的单片机设计与实现 46513.2.1 ATMEL AT90S4433单片机及其开发系统 46513.2.2 联机电话防火墙的功能 46813.2.3 联机电话防火墙的原理及其实现 46913.3 电信固定网虚拟专网 47113.3.1 电信固定网VPN的体系结构 47113.3.2 一种基于DSP的电信固定网VPN(替音电话) 47213.3.3 替音电话算法的仿真结果

<<网络安全理论与技术>>

47613.4 电信固定网入侵检测 48313.4.1 电信固定网的常见攻击手段 48413.4.2 电话盗用攻击的检测 48513.4.3 搭线窃听攻击的检测 487第14章 安全移动通信系统 48914.1 GSM安全机制 48914.1.1 移动通信面临的安全威胁 48914.1.2 GSM系统的安全机制 49014.1.3 GSM系统的安全缺陷 49214.2 GPRS安全机制 49214.2.1 GPRS系统的网络结构 49214.2.2 GPRS系统的安全机制 49314.2.3 GPRS系统的安全缺陷 49514.3 3G安全机制 49614.3.1 安全结构 49714.3.2 网络接入安全机制 49914.3.3 接入链路数据完整性 50314.3.4 接入链路数据保密性 50414.3.5 密钥管理 506第15章 安全短信系统 51115.1 短消息服务与安全需求 51115.1.1 短消息服务的系统结构 51115.1.2 短消息服务的安全需求与现状 51215.1.3 SIM卡执行环境 51315.2 基于短消息的移动电子商务安全协议 51515.2.1 基于短消息的移动电子商务安全需求 51515.2.2 基于短消息的身份认证协议 51615.2.3 移动电子商务的反拒认协议 52215.3 基于SIM卡的电子支付协议 53015.3.1 设计目的 53015.3.2 协议内容 53115.3.3 协议分析 54215.4 短消息应用系统实例 54315.4.1 业务简介 54315.4.2 系统结构 54315.4.3 应用系统的实现 544第16章 安全邮件系统 55016.1 电子邮件系统简介 55016.1.1 电子邮件系统的收发机制 55016.1.2 电子邮件的一般格式 55116.2 电子邮件系统的安全问题 55216.2.1 电子邮件的安全需求 55216.2.2 基于应用层的安全电子邮件 55316.2.3 基于网络层的安全电子邮件 55316.3 安全电子邮件系统实例 55416.3.1 IP包的检测流程 55416.3.2 IP包传送的不对称性 55516.3.3 TCP段的重传机制 55616.3.4 加密后的IP包数据的编码问题 55716.3.5 E-mail发送失败的一个例子 55716.3.6 发送邮件时TCP段序列号的修正方案 55716.3.7 Base64编码 56216.3.8 邮件接收时的TCP段序列号处理方案 56316.3.9 密钥管理 565 参考文献 567

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>