

<<网络安全设计>>

图书基本信息

书名：<<网络安全设计>>

13位ISBN编号：9787115136930

10位ISBN编号：7115136939

出版时间：2005-9

出版时间：人民邮电出版社

作者：凯

页数：516

字数：842000

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>

<<网络安全设计>>

内容概要

本书第一版曾在2000年译成中文，受到读者的普遍欢迎。

本书在第一版的基础上，增加了许多有关计算机网络安全技术的新发展的内容，并增加了在虚拟专用网、无线网与VoIP网中解决有关实际问题的章节，还增加了一章内容集中讲述路由协议安全。

此外，本书还补充了许多关于防火墙和入侵检测系统等主题的内容。

本书共包括4个部分：第一部分由基本密码学、网络安全技术、安全技术在实际网络中的应用、路由协议安全等内容组成，以便读者掌握技术背景；第二部分由企事业网络中存在的威胁、网络站点安全策略的考虑、企事业网络安全策略的设计与实现、安全事故的处理等内容组成，帮助读者掌握创建网络安全策略所需的相关知识；第三部分则由确保企事业网络基础设施安全、确保Internet访问的安全、确保远程接入的安全，以及确保虚拟专用网、无线网和VoIP网安全等内容组成，为读者展示了如何使用思科设备构建网络安全性的综合设计思路和实例；第四部分是一组附录，列出了可以从中获得更多关于网络安全性设计的技术信息的资源，包括安全意外事故处理和减轻分布式拒绝服务攻击(DdoS)的方法和步骤等内容。

此外，本书最后还附有术语表、各章的习题解答，供读者参考。

本书适用于从事计算机网络安全的设计、管理、维护的设计师、工程师和架构师等工程技术人员学习，也可作为高等院校计算机和通信专业的本科生和研究生学习计算机网络信息安全方面课程的教材或参考书。

<<网络安全设计>>

作者简介

Merike Kaeo, CCIE No.1287, 目前主要从事与安全有关的产品和网络设计方案的咨询工作。她从事网络领域的工作超过15年, 1988年到1993年期间在Bethesda的NIH(国家卫生研究中心)工作, 她使用思科路由器来设计并实现了NIH最初的FDDI骨干网络。从1993年到2000年她任职于思科公司, 主要从事路由器的性能、路由协议、网络设计、网络安全等相关技术工作。她是思科公司安全领域中的主要成员, 也是公司的安全技术顾问和各种安全相关的会议演讲人。她于1987年从Rutgers大学获得电子工程学士学位, 并于1998年从乔治华盛顿大学获得电子工程硕士学位。

<<网络安全设计>>

书籍目录

- 第一部分 安全基础第1章 基本密码学 31.1 密码学 31.1.1 对称密钥加密 41.1.2 非对称加密
81.1.3 哈希函数 111.1.4 数字签名 121.2 认证和授权 141.2.1 认证方式 141.2.2 信任模型
141.3 命名空间 151.4 密钥管理 161.4.1 创建和分配密钥 161.4.2 创建和分配公钥 191.5
密钥托管 211.5.1 商业情况 221.5.2 政治角度(美国) 221.5.3 人为因素 221.6 小结 231.7 复
习题 23第2章 安全技术 272.1 身份技术 282.1.1 安全口令 282.1.2 PPP(点对点)认证协议
322.1.3 使用认证机制的协议 392.2 应用层安全协议 522.2.1 SHTTP 522.2.2 S/MIME 532.3
传输层安全协议 552.3.1 安全套接层/传输层安全协议 552.3.2 SSH协议 582.3.3 套接
字(SOCKS)协议 592.4 网络层安全 602.5 数据链路层安全技术 752.5.1 二层转发协议 752.5.2
点对点隧道协议 772.5.3 二层隧道协议 792.5.4 PPPoE 832.6 公钥体制和分配模型 842.6.1
PKI的功能 852.6.2 使用PKI的场景实例 862.6.3 证书 862.6.4 X.509标准 872.6.5 证书分发
892.7 小结 892.8 复习题 90第3章 安全技术在实际网络中的应用 933.1 虚拟专用网(VPN)
933.1.1 VPN调度模型 933.1.2 VPN安全 963.1.3 访问VPN 1033.1.4 内部网/外部网的VPN
1043.2 无线网络 1043.2.1 无线技术的类型 1053.2.2 无线局域网组件 1063.2.3 无线局域网调
度模型 1063.2.4 802.11物理层基础知识 1083.2.5 无线局域网(WLAN)安全 1143.3 VoIP网络
1223.3.1 IP电话网组件 1233.3.2 IP电话调度模型 1233.3.3 VoIP协议 1243.3.4 介质网关控制
协议(MGCP) 1293.3.5 初始会话协议(SIP) 1293.3.6 VoIP安全协议 1333.3.7 VoIP安全解决方案
1383.4 小结 1393.5 复习题 140第4章 路由协议安全 1434.1 路由基本知识 1434.1.1 路由
协议分类 1444.1.2 路由协议安全性 1454.2 路由协议安全细节 1484.2.1 RIP 1484.2.2 EIGRP
1534.2.3 OSPF 1554.2.4 IS-IS 1594.2.5 BGP-4 1624.3 小结 1634.4 复习题 164第二部分
企业安全策略第5章 企业网中的威胁 1695.1 威胁的类型 1705.1.1 未授权的访问 1705.1.2 假
冒 1755.1.3 拒绝服务 1785.1.4 DDoS(分布式拒绝服务攻击) 1785.2 威胁的动机 1815.3 常见
协议的脆弱性 1815.3.1 TCP/IP协议 1825.3.2 UDP协议 1865.3.3 ICMP协议 1865.3.4 DNS协
议 1885.3.5 NNTP协议 1915.3.6 SMTP协议 1915.3.7 FTP协议 1925.3.8 远程过程调用(RPC)
服务 1925.3.9 NFS/NIS服务 1935.3.10 X Window系统 1945.4 常见网络方案威胁和脆弱性
1945.4.1 虚拟专用网 1945.4.2 无线网络 1965.4.3 IP上的语音网(VoIP) 1995.5 路由协议
2025.6 社会工程 2035.7 小结 2035.8 复习题 203第6章 站点安全策略的注意事项 2076.1
何处入手 2086.2 风险管理 2096.2.1 评估风险 2106.2.2 风险缓解和安全成本 2146.3 安全策
略框架 2166.3.1 企业网的组成部分 2166.3.2 安全体系结构的要素 2176.3.3 其他考虑的因素
2196.4 小结 2206.5 复习题 220第7章 企业安全策略的设计与实施 2237.1 物理安全控制
2247.1.1 物理网络基础设施 2247.1.2 物理设备安全性 2277.1.3 物理安全控制策略实例 2297.2
逻辑安全控制 2307.2.1 子网边界 2307.2.2 逻辑访问控制 2357.2.3 逻辑安全控制策略实例
2377.3 基础设施和数据完整性 2387.3.1 防火墙 2387.3.2 网络服务 2407.3.3 经认证的数据
2417.3.4 常见攻击的防范 2427.3.5 基础设施和数据完整性策略实例 2437.4 数据机密性
2437.5 安全策略验证与监控 2447.5.1 脆弱性扫描器 2447.5.2 账户管理 2447.5.3 安全管理
2447.5.4 入侵检测 2457.5.5 验证和监控部分实例 2467.6 为员工制定的策略和步骤 2477.6.1
安全备份 2477.6.2 设备认证 2477.6.3 使用便携工具 2477.6.4 审计跟踪 2487.6.5 员工策略和
步骤实例 2497.7 安全意识培训 2497.8 小结 2507.9 复习题 250第8章 事故处理 2538.1 建
立事故响应小组 2558.2 检测事故 2568.2.1 跟踪重要信息 2568.2.2 入侵检测系统 2568.3 处
理事故 2608.3.1 重点采取的行为 2608.3.2 评估事故损害 2618.3.3 报告和报警过程 2618.4 减
少事故脆弱性 2628.5 对事故的响应 2638.5.1 保存准确的文档记录 2638.5.2 现实世界中的实例
2638.6 从事故中恢复 2648.7 小结 2658.8 复习题 265第三部分 具体的实现第9章 确保企
业网络基础设施的安全 2699.1 身份——控制网络设备的访问 2709.1.1 基本访问和特权访问
2709.1.2 线路访问控制 2829.2 完整性 2919.2.1 映像认证 2929.2.2 安全工作组 2929.2.3
路由认证 2939.2.4 路由过滤器和路由可信度 2949.3 数据机密性 2969.4 网络可用性 2979.4.1
冗余功能 2979.4.2 防范常见的攻击 3039.5 审计 3059.5.1 确认配置 3059.5.2 监控和记录网

<<网络安全设计>>

络活动 3069.5.3 入侵检测 3089.5.4 进一步的讨论 3119.6 实现的范例 3119.7 小结 3179.8
复习题 317第10章 确保因特网访问安全 32110.1 因特网访问体系结构 32110.2 外部屏蔽路由器
体系结构 32310.3 高级防火墙体系结构 33110.3.1 高级报文分组会话过滤 33210.3.2 应用内容
过滤 33310.3.3 URL过滤/隔离 33310.3.4 电子邮件和SMTP 33310.3.5 其他常用的应用协议
33410.3.6 应用认证/授权 33610.3.7 加密 33710.3.8 网络地址转换 34010.4 实现的范例
34210.4.1 Cisco IOS防火墙 34210.4.2 PIX防火墙 34910.5 小结 35910.6 复习题 359第11章
确保远程拨入访问的安全 36311.1 拨号接入的安全性因素 36411.2 认证拨号接入的用户和设备
36511.2.1 简单拨号接入环境 36511.2.2 复杂拨号接入环境 37011.3 授权 37411.4 账户管理
和记账 37911.4.1 TACACS+和RADIUS账户管理 37911.4.2 集中记账 38011.5 使用AAA的特殊
功能 38211.5.1 锁和密钥功能 38211.5.2 双重认证/授权 38711.6 为虚拟拨号接入环境提供加密
39311.6.1 GRE隧道和CET 39311.6.2 IPSec 40011.6.3 带有IPSec的L2TP 40511.7 小结
42011.8 复习题 420第12章 确保VPN、无线网络及VoIP网络的安全 42312.1 虚拟专用网(VPN)
42312.1.1 身份 42512.1.2 完整性 43312.1.3 机密性 43312.1.4 可用性 43312.1.5 审计
43412.1.6 VPN设计实例 43412.2 无线网络 43512.2.1 身份 43612.2.2 完整性 43712.2.3 机
密性 43712.2.4 可用性 43712.2.5 审计 43812.2.6 无线网络设计实例 43812.3 IP语音网
络(VoIP) 43912.3.1 身份 43912.3.2 完整性 44312.3.3 机密性 44312.3.4 可用性 44412.3.5 审
计 44412.3.6 VoIP网络设计参考 44512.4 小结 44512.5 复习题 445第四部分 附录附录A 技
术信息资源 449附录B 报告和预防指南：工业间谍和网络入侵 453附录C 端口号 465附录D 缓
减分布式拒绝服务攻击 469附录E 复习题答案 495术语表 509

<<网络安全设计>>

媒体关注与评论

本书是一本实用指南，有助于你理解保证企业网络基础设施安全的基本原理。本书综合介绍了基本安全技术、创建安全策略的过程和实施企业安全策略的实际需要。

你将透彻理解基本密码学——一种常见的安全技术以及新近出现的关键安全技术。通过了解可能的威胁和脆弱性、理解实施风险管理评估所需要的步骤，你将能够指导企业环境中安全策略的构建和实施。

通过具体配置实例的应用，可以了解为实现给定安全策略而配置的网络基础设施设备所需要的性能，这些策略保证企业内部基础设施、因特网接入和远程接入环境的安全。

这一新版中涵盖了新的安全性能，包括用于路由器、交换机的SSH和PIX防火墙；对L2TP和IPSEC的增强；针对无线网络的CISCO LEAP；数字证书，先进的AAA功能；CISCO入侵检测系统的性能和产品等。

另外也提供了一些有关当前安全发展趋势的实际例子，包括VPN、无线和VOIP网络实例。

<<网络安全设计>>

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>