第一图书网, tushu007.com

<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787302270683

10位ISBN编号：7302270686

出版时间：2011-12

出版时间：清华大学出版社

作者：姚永雷，马利　主编

页数：229

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

第一图书网, tushu007.com

<<计算机网络安全>>

内容概要

本书是《计算机网络安全》（马利主编，清华大学出版社出版）的修订本，在第一版基础上做了大量的修改，既注重介绍网络安全基础理论，又着眼培养读者网络安全技术和实践能力。
全书详细讨论了密码学、消息鉴别和数字签名、身份认证技术、internet的安全技术、恶意代码及其防杀技术、防火墙、网络攻击与防范技术、虚拟专用网技术等计算机网络安全的相关理论和主流技术。

本书的编写思路是理论与实践相结合，一方面强调基本概念、理论、算法和协议的介绍，另一方面重视技术和实践，力求在实践中深化理论。
希望通过本书的介绍，让读者既能掌握完整、系统的计算机网络安全理论，又具备运用主流网络安全技术实现安全网络的设计能力。

本书是一本理想的计算机专业本科生、大专生的计算机网络安全教材，对从事计算机网络安全工作的工程技术人员，也是一本非常好的参考书。

第一图书网, tushu007.com

<<计算机网络安全>>

书籍目录

第1章概述
1.1网络安全面临的挑战
1.2网络安全的基本概念
1.2.1网络安全的定义
1.2.2网络安全的属性
1.2.3网络安全层次结构
1.2.4网络安全模型
1.3osi安全体系结构
1.3.1安全攻击
1.3.2安全服务
1.3.3安全机制
1.4网络安全防护体系
1.4.1网络安全策略
1.4.2网络安全体系
思考题
第2章密码学
2.1密码学概述
2.1.1密码学的发展
2.1.2密码学的基本概念
2.1.3密码的分类
2.2古典密码体制
2.2.1置换技术
2.2.2代换技术
2.2.3古典密码分析
2.2.4一次一密
2.3对称密码体制
2.3.1对称密码体制的概念
2.3.2des
2.3.3其他算法简介
2.4公钥密码体制
2.4.1公钥密码体制原理
2.4.2rsa算法
2.4.3elgamal公钥密码体制
2.5密钥管理
2.5.1公钥分配
2.5.2对称密码体制的密钥分配
2.5.3公钥密码用于对称密码体制的密钥分配
2.5.4diffie?hellman密钥交换
思考题
第3章消息鉴别与数字签名
3.1消息鉴别
3.1.1消息鉴别的概念
3.1.2基于mac的鉴别
3.1.3基于散列函数的鉴别
3.1.4散列函数

第一图书网, tushu007.com

3.2数字签名
3.2.1数字签名简介
3.2.2基于公钥密码的数字签名原理
3.2.3数字签名算法
思考题
第4章身份认证
4.1用户认证
4.1.1基于口令的认证
4.1.2基于智能卡的认证
4.1.3基于生物特征的认证
4.2认证协议
4.2.1单向认证
4.2.2双向认证
4.3kerberos
4.3.1kerberos版本4
4.3.2kerberos版本5
4.4x.509认证服务
4.4.1证书
4.4.2认证过程
4.4.3x.509版本3
4.5公钥基础设施
4.5.1pki体系结构
4.5.2认证机构
4.5.3pkix相关协议
4.5.4pki信任模型
思考题
第5章internet安全
5.1ip安全
5.1.1ipsec体系结构
5.1.2ipsec工作模式
5.1.3ah协议
5.1.4esp协议
5.1.5ike
5.2ssl/tls
5.2.1ssl体系结构
5.2.2ssl记录协议
5.2.3ssl修改密码规范协议
5.2.4ssl报警协议
5.2.5ssl握手协议
5.2.6tls
5.3pgp
5.3.1pgp操作
5.3.2pgp密钥
5.4internet欺骗
5.4.1arp欺骗
5.4.2dns欺骗
5.4.3ip地址欺骗

第一图书网, tushu007.com

5.4.4web欺骗
思考题
第6章恶意代码
6.1恶意代码的概念及关键技术
6.1.1恶意代码的概念
6.1.2恶意代码生存技术
6.1.3恶意代码隐藏技术
6.2计算机病毒
6.2.1计算机病毒概述
6.2.2计算机病毒防治技术
6.3木马
6.3.1木马概述
6.3.2木马的工作原理
6.3.3木马防治技术
6.4蠕虫
6.4.1蠕虫概述
6.4.2蠕虫的传播过程
6.4.3蠕虫的分析和防范
6.5其他常见恶意代码
思考题
第7章防火墙
7.1防火墙的概念
7.2防火墙的特性
7.3防火墙的技术
7.3.1包过滤技术
7.3.2代理服务技术
7.3.3状态检测技术
7.3.4自适应代理技术
7.4防火墙的体系结构
7.5个人防火墙
7.6防火墙的应用与发展
7.6.1防火墙的应用
7.6.2防火墙技术的发展
思考题
第8章网络攻击与防范
8.1网络攻击概述
8.1.1网络攻击的概念
8.1.2网络攻击的类型
8.1.3网络攻击的过程
8.2常见网络攻击
8.2.1拒绝服务攻击
8.2.2分布式拒绝服务攻击
8.2.3缓冲区溢出攻击
8.3入侵检测
8.3.1入侵检测概述
8.3.2入侵检测系统分类
8.3.3分布式入侵检测

第一图书网, tushu007.com

8.3.4入侵检测技术发展趋势
8.4计算机紧急响应
8.4.1紧急响应
8.4.2蜜罐技术
思考题
第9章虚拟专用网
9.1vpn概述
9.1.1vpn的概念
9.1.2vpn的基本类型
9.1.3vpn的实现技术
9.1.4vpn的应用特点
9.2隧道技术
9.2.1隧道的概念
9.2.2隧道的基本类型
9.3实现vpn的二层隧道协议
9.3.1pptp
9.3.2l2f
9.3.3l2tp
9.4实现vpn的三层隧道协议
9.4.1gre
9.4.2ipsec
9.5mpls vpn
9.5.1mpls的概念和组成
9.5.2mpls的工作原理
9.5.3mpls vpn的概念和组成
9.5.4mpls vpn的数据转发过程
9.6ssl vpn
9.6.1ssl vpn概述
9.6.2基于web浏览器模式的ssl vpn
9.6.3ssl vpn的应用特点
思考题

第一图书网, tushu007.com

章节摘录

版权页：插图：对称密码要求消息交换的双方共享密钥，并且此密钥不为他人所知。
此外，密钥要经常变动，以防攻击者知道。
因此，任何密码系统的强度都与密钥分配方法有关。
对于参与者A和B，密钥的分配有以下几种办法：（1）密钥由A选择，并亲自交给B。
（2）第三方C选择密钥后亲自交给A和B。
（3）如果A和B以前或最近使用过某密钥，其中一方可以用它加密一个新密钥后再发送给另一方。
（4）A和B与第三方C均有秘密渠道，则C可以将一密钥分别秘密发送给A和B。
方法（1）和方法（2）需要人工传送密钥，适用于密钥数目较少且距离不远的情况，比如链路加密，因为每个链路加密设备仅同链路另一方进行数据交换。
但人工传送不适于端对端加密。
在分布式系统，特别是那些广域分布系统中，某一主机可能需要和其他任何主机经常交换数据，需要大量动态产生的密钥。
方法（3）既可用于链路加密，也可用于端对端加密。
但是如果攻击者曾经成功地获取一个密钥，则所有的子密钥都暴露了。
此外，成千上万个初始密钥的分发也是一个困难。
假设方法（4）中的第三方是一个密钥分配中心，负责分发密钥给需要的用户（主机、进程、应用）。
每个用户与密钥分配中心共享一个密钥，此密钥用于密钥分配。
这种方式可应用于端到端加密。
典型的密钥分配模式如图2-17所示。

第一图书网, tushu007.com

<<计算机网络安全>>

编辑推荐

《计算机网络安全(第2版)》编辑推荐：教育部高等学校软件工程专业教学指导分委员会推荐教材，根据教育部“软件工程课程体系研究”项目成果《中国软件工程学科教程》及专业规范组织编写，与最新ACM和IEEE CCSE同步，汇集示范性软件工程专业教学成果。

第一图书网, tushu007.com

<<计算机网络安全>>

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