

<<网络信息安全技术>>

图书基本信息

书名：<<网络信息安全技术>>

13位ISBN编号：9787560624488

10位ISBN编号：7560624480

出版时间：2010-8

出版时间：周明全、吕林涛、李军怀、等 西安电子科技大学出版社 (2010-08出版)

作者：周明全 等著

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>

<<网络信息安全技术>>

内容概要

《网络信息安全技术（第2版）》是一本计算机网络安全方面的专业教材，主要介绍了网络安全的基础理论和关键技术。

本书遵循理论与实际相结合的原则，既注重基本原理、概念的准确严谨，又关注技术内容的新颖和先进性。

《网络信息安全技术（第2版）》是在第一版的基础上修订的，增加了黑客攻击和防范技术、网络漏洞扫描技术，删除了“代理服务及应用”一章。

《网络信息安全技术（第2版）》共分为12章，内容包括网络安全概述、密码技术、密钥管理技术、数字签名与认证技术、黑客攻击和防范技术、网络漏洞扫描技术、网络入侵检测原理与技术、Internet基础设施的安全性、电子商务的安全技术及应用、包过滤技术原理及应用、防火墙技术以及信息隐藏技术。

为配合教学，书中各章后均附有习题，以帮助学习者加深对书中内容的理解。

本书附录中给出了近年来国家有关部门颁布的网络安全相关法规，读者可结合需要参考使用。

《网络信息安全技术（第2版）》力求为读者展现目前计算机网络安全的新技术，内容具有系统性和实用性的特点，语言叙述通俗易懂，并精心设计了大量图表，易于理解。

《网络信息安全技术（第2版）》可作为高等学校计算机及相关专业本科生或研究生的教材，也可作为网络信息安全领域专业人员的参考书。

书籍目录

第1章网络安全概述 1.1网络安全的基础知识 1.1.1网络安全的基本概念 1.1.2网络安全的特征 1.1.3网络安全的目标 1.1.4网络安全需求与安全机制 1.2威胁网络安全的因素 1.2.1网络的安全威胁 1.2.2网络安全的问题及原因 1.3网络安全防护体系 1.3.1网络安全策略 1.3.2网络安全体系 1.4网络安全的评估标准 1.4.1可信计算机系统评价准则简介 1.4.2安全标准简介 习题1 第2章密码技术 2.1密码技术的基本概念 2.2古典密码体制 2.2.1置换密码 2.2.2代换密码 2.3对称密码体系 2.3.1流密码 2.3.2分组密码 2.3.3数据加密标准 (DES) 2.3.4高级加密标准 (AES) 2.4公钥 (非对称) 密码体制 2.4.1公钥密码体制的基本概念 2.4.2公钥密码体制的原理 2.4.3RSA算法 2.4.4RSA算法中的计算问题 2.4.5RSA算法的安全性 2.4.6RSA算法的实用性及数字签名 2.4.7RSA算法和DES算法的特点 2.5椭圆曲线密码体制 2.5.1椭圆曲线 2.5.2有限域上的椭圆曲线 2.5.3椭圆曲线上的密码 习题2 第3章密钥管理技术 3.1密钥的管理概述 3.1.1密钥的生成与分配 3.1.2密钥的保护与存储 3.1.3密钥的有效性与使用控制 3.2密钥的分类 3.3密钥分配技术 3.3.1密钥分配实现的基本方法和基本工具 3.3.2密钥分配系统实现的基本模式 3.3.3密钥的验证 3.4公开密钥基础设施 (PKI) 3.4.1PKI概述 3.4.2公钥密码体制的原理与算法 3.4.3公钥证书 3.4.4公钥证书的管理 3.4.5PKI信任模型 习题3 第4章数字签名与认证技术 4.1数字签名概述 4.1.1数字签名的概念 4.1.2数字签名技术应满足的要求 4.1.3数字签名的原理 4.1.4数字签名技术 4.2数字签名标准及数字签名算法 4.2.1DSS与RSA的比较 4.2.2数字签名算法DSA 4.2.3数字签名算法Hash 4.2.4数字签名算法RSA 4.3其他数字签名体制 4.3.1基于离散对数问题的数字签名体制 4.3.2基于大数分解问题的数字签名体制 4.4散列函数与消息认证 4.4.1散列函数的定义及性质 4.4.2散列函数的结构 4.4.3安全散列函数 (SHA) 4.4.4消息认证 4.5认证及身份验证技术 4.5.1单向认证技术 4.5.2交叉认证技术 4.5.3身份验证技术 4.5.4身份认证系统实例——Kerberos系统 4.5.5X.509认证技术 习题4 第5章黑客攻击和防范技术 5.1黑客攻击及其原因 5.1.1黑客及其起源 5.1.2黑客入侵与攻击 5.1.3黑客攻击的动机及其成功的原因 5.2黑客攻击的流程 5.2.1网络踩点 5.2.2网络扫描 5.2.3黑客查点 5.2.4获取访问权 5.2.5权限提升 5.2.6窃取信息 5.2.7清除痕迹 5.2.8创建后门 5.2.9拒绝服务攻击 5.3黑客攻击技术分析 5.3.1协议漏洞渗透 5.3.2密码分析还原 5.3.3应用漏洞分析与渗透 5.3.4社会工程学方法 5.3.5恶意拒绝服务攻击 5.3.6病毒或后门攻击 5.4网络环境下的攻击 5.4.1针对远程接入的攻击 5.4.2针对防火墙的攻击 5.4.3网络拒绝服务攻击 习题5 第6章网络漏洞扫描技术 6.1计算机网络漏洞概述 6.1.1存在漏洞的原因 6.1.2漏洞信息的获取 6.2漏洞检测策略 6.3常用扫描工具 6.3.1X - Scan 6.3.2Nmap 6.3.3Nessus 6.3.4SATAN 6.3.5SAINT 6.3.6SARA 6.3.7ISS 6.3.8Retina 6.3.9GFILANguardNSS 6.3.10SSS 6.3.11MBSA 6.4漏洞扫描的实施 6.4.1发现目标 6.4.2摄取信息 6.4.3漏洞检测 6.5小结 习题6 第7章网络入侵检测原理与技术 7.1入侵检测原理 7.1.1入侵检测的概念 7.1.2入侵检测模型 7.1.3IDS在网络中的位置 7.2入侵检测方法 7.2.1基于概率统计的检测 7.2.2基于神经网络的检测 7.2.3基于专家系统的检测 7.2.4基于模型推理的检测 7.2.5基于免疫的检测 7.2.6入侵检测新技术 7.2.7其他相关问题 7.3入侵检测系统 7.3.1入侵检测系统的构成 7.3.2入侵检测系统的分类 7.3.3基于主机的入侵检测系统HIDS 7.3.4基于网络的入侵检测系统NIDS 7.3.5分布式入侵检测系统 7.4入侵检测系统的测试评估 7.4.1测试评估概述 7.4.2测试评估的内容 7.4.3测试评估标准 7.4.4IDS测试评估现状以及存在的问题 7.5典型的IDS系统及实例 7.5.1典型的IDS系统 7.5.2入侵检测系统实例Snort 7.6入侵防护系统 7.6.1IPS的原理 7.6.2IPS的分类 7.6.3IPS和IDS的比较 7.7入侵检测技术的发展方向 习题7 第8章Internet基础设施的安全性 8.1Internet安全概述 8.2DNS的安全性 8.2.1目前DNS存在的安全威胁 8.2.2Windows下的DNS欺骗 8.2.3拒绝服务攻击 8.3安全协议IPSec 8.3.1IP协议简介 8.3.2下一代IP——IPv6 8.3.3IP安全协议IPSec的用途 8.3.4IPSec的结构 8.4电子邮件的安全性 8.4.1PGP 8.4.2S/MIME 8.5Web的安全性 8.5.1Web的安全性要求 8.5.2安全套接字层 (SSL) 8.5.3安全超文本传输协议 8.6虚拟专用网及其安全性 8.6.1VPN简介 8.6.2VPN协议 8.6.3VPN方案设计 8.6.4VPN的安全性 8.6.5微软的点对点加密技术 8.6.6第二层隧道协议 8.6.7VPN发展前景 习题8 第9章电子商务的安全技术及应用 9.1电子商务概述 9.1.1电子商务的概念 9.1.2电子商务的分类 9.1.3电子商务系统的支持环境 9.2电子商务的安全技术要求 9.2.1电子商务与传统商务的比较 9.2.2电子商务面临的威胁和安全技术要求 9.2.3电子商务系统所需的安全服务 9.2.4电子商务的安全体系结构 9.3电子支付系统的安全技术 9.3.1电子支付系统的安全要求 9.3.2电子支付手段 9.4电子现金应用系统 9.4.1电子现金应用系统的安全技术 9.4.2脱机实现方式中的密码技术 9.4.3电子钱包 9.5电子现金协议技术 9.5.1不可跟踪的电子现金协议技术

9.5.2可分的电子现金协议技术 9.5.3基于表示的电子现金协议技术 9.5.4微支付协议技术 9.5.5可撤销匿名性的电子现金系统实现技术 9.6电子商务应用系统实例 9.6.1某海关业务处理系统 9.6.2某海关电子申报系统网络平台 9.6.3某海关电子申报系统的软件体系结构 习题9 第10章包过滤技术原理及应用 10.1高层IP网络的概念 10.2包过滤的工作原理 10.2.1包过滤技术传递的判据 10.2.2包过滤技术传递操作 10.2.3包过滤方式的优缺点 10.3包过滤路由器的配置 10.3.1协议的双向性 10.3.2“往内”与“往外” 10.3.3“默认允许”与“默认拒绝” 10.4包的基本构造 10.5包过滤处理内核 10.5.1包过滤和网络策略 10.5.2一个简单的包过滤模型 10.5.3包过滤器操作 10.5.4包过滤设计 10.6包过滤规则 10.6.1制订包过滤规则应注意的事项 10.6.2设定包过滤规则的简单实例 10.7依据地址进行过滤 10.8依据服务进行过滤 10.8.1往外的Telnet服务 10.8.2往内的Telnet服务 10.8.3Telnet服务 10.8.4有关源端口过滤问题 习题10 第11章防火墙技术 11.1防火墙的概念 11.2防火墙的原理及实现方法 11.2.1防火墙的原理 11.2.2防火墙的实现方法 11.3防火墙体系结构 11.3.1双宿主主机体系结构 11.3.2堡垒主机过滤体系结构 11.3.3过滤子网体系结构 11.3.4应用层网关体系结构 11.4防火墙的构成 11.4.1防火墙的类型及构成 11.4.2防火墙的配置 11.5防火墙所采用的技术及其作用 11.5.1隔离技术 11.5.2管理技术 11.5.3防火墙操作系统的技术 11.5.4通信堆叠技术 11.5.5网络地址转换技术 11.5.6多重地址转换技术 11.5.7虚拟私有网络技术 (VPN) 11.5.8动态密码认证技术 11.6防火墙选择原则 11.6.1防火墙安全策略 11.6.2选择防火墙的原则 11.7防火墙建立实例 11.7.1包过滤路由器的应用 11.7.2屏蔽主机防火墙的应用 11.7.3屏蔽子网防火墙的应用 11.7.4某企业防火墙建立实例 习题11 第12章信息隐藏技术 12.1信息隐藏概述 12.1.1信息隐藏的基本概念 12.1.2信息隐藏的基本过程 12.2信息隐藏技术的分类及应用领域 12.2.1信息隐藏的分类 12.2.2信息隐藏技术的应用领域 12.3数字图像水印技术 12.3.1数字水印技术的基本原理 12.3.2空域图像水印技术 12.3.3频域图像水印技术 12.4数字文本水印技术 12.4.1数字文本水印技术原理 12.4.2行移编码 12.4.3字移编码 12.4.4特征编码 12.4.5编码方式的综合运用 12.5数字语音水印技术 12.5.1最不重要位 (LSB) 方法 12.5.2小波变换方法 12.6数字视频水印技术 12.6.1数字视频水印技术的一般原理 12.6.2原始视频水印 12.6.3压缩视频水印 习题12 附录A《中华人民共和国计算机信息网络国际联网管理暂行办法》 附录B《中华人民共和国计算机信息网络国际联网安全保护管理办法》 附录C《中华人民共和国计算机信息系统安全保护条例》 参考文献

章节摘录

版权页：插图：公开密钥密码体制也称为非对称密码体制，是现代密码学中革新性的研究成果和重要进展。

公开密钥算法于1976年由美国斯坦福大学的迪菲（Diffie）和赫尔曼（Hellman）提出，公开密钥密码体制的原理是加密过程中使用不相同的加密密钥和解密密钥，并且无法从其中一个密钥推算出另一个

。公开密钥密码的优点是不需要传递用户私人的解密密钥，简化了密钥管理。

公钥体制采用的算法有时也称为公开密钥算法（或简称为公钥算法）。

非对称密码体制的安全性取决于所采用的难以解决的数学问题是否会被攻破，大整数因式分解是一种常用手段。

2.4.1 公钥密码体制的基本概念 公钥体制下，一个用户可以将自己设计的加密公钥和加密算法对外公布，而只保留解密用的私钥。

任何人都可以获取这个用户的加密公钥和加密算法，并向该用户发送加密过的信息，该用户接收后可以使用私钥还原消息。

在这个公钥加解密的过程中，会涉及到公私密钥对、数字证书以及电子签证机关等主要内容。

1. 密钥对 在基于公钥体系的安全加密系统中，密钥生成过程每次都产生一个公钥和一个私钥，形成加密和解密的密钥对。

在实际应用中，私钥由用户私人保存，而公钥则通过某种手段对外公布。

公钥体系的基础问题是公钥的分发与管理，这是电子商务等业务系统能够广泛应用的基础。

一个集体如果成员之间可以互信，比如A和B两人形成小集体，他们之间完全互信并直接交换公钥，在互联网上进行保密通信，不存在密钥和身份安全问题。

这个集体再稍微扩大一点，成员之间有基本的信任关系，虽然从法律角度讲这种信任有一定风险，但通常也可以完成安全通信。

如果在开放环境下，如互联网环境下，通信双方缺乏基本的信任关系，并且存在大量的恶意用户，密钥和身份的信任问题就成了一个大问题。

2. 数字证书 公开密钥体系需要在开放环境下使用，公钥加密体系采取将公钥和公钥的主人名字联系在一起的方法，再请一个有信誉的公正权威机构对每个公钥和所有者身份进行确认，确认后的公钥信息加上这个权威机构的签名，就形成了数字证书，也称为证书。

由于证书上有权威机构的签字，因此人们公认证书上的内容是可信任的；又由于证书上有主人的名字等身份信息，别人就能很容易地知道公钥的主人是谁。

有了数字证书之后，互联网上的庞大用户群之间可以通过权威机构建立起基本的信任关系，使得彼此都不能轻易信任的用户之间可以完成通信。

证书就是用户在网上的电子个人身份证，在电子商务中的作用同日常生活中使用的个人身份证作用一样。

<<网络信息安全技术>>

编辑推荐

《普通高等教育"十一五"国家级规划教材:网络信息安全技术(第2版)》力求为读者展现目前计算机网络安全的新技术,内容具有系统性和实用性的特点,语言叙述通俗易懂,并精心设计了大量图表,易于理解。

《普通高等教育"十一五"国家级规划教材:网络信息安全技术(第2版)》可作为高等学校计算机及相关专业本科生或研究生的教材,也可作为网络信息安全领域专业人员的参考书。

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>