<<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

<<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。

<<网络信息安全技术>>

书籍目录

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。

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。

<<网络信息安全技术>>

版权说明