<<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：9787302217350

10位ISBN编号：7302217351

出版时间：2010-8

出版时间：清华大学出版社

作者：马利，姚永雷　主编

页数：250

前言

在全球信息化的背景下，信息已成为一种重要的战略资源。
信息的应用涵盖国防、政治、经济、科技、文化等各个领域，在社会生产和生活中的作用愈来愈显著。
随着Internet在全球的普及和发展，计算机网络成为信息的主要载体之一。
信息网络技术的应用愈加普及和广泛，应用层次逐步深入，应用范围不断扩大。
国家发展和社会运转，以及人类的各项活动对计算机网络的依赖性越来越强。
另一方面，计算机网络的全球互联趋势愈来愈明显，人类活动对计算机网络的依赖性不断增大，基于网络的应用层出不穷，也使得网络安全问题更加突出，受到越来越广泛的关注。
计算机网络的安全性已成为当今信息化建设的核心问题之一。
网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。
网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。
全书内容安排如下：（1）第1章着重讨论了目前存在的网络安全挑战；介绍了网络安全的定义、网络安全的属性、网络安全层次结构、网络安全模型；在介绍OSI安全体系结构中主要关注了安全攻击、安全机制和安全服务；网络安全防护体系的建立是基于安全技术的集成基础之上，依据一定的安全策略建立起来的，在介绍时侧重了网络安全策略和网络安全体系。
（2）密码是通信双方按约定的法则对信息进行特定变换的一种重要保密手段。
密码学是实现网络安全服务和安全机制的基础，是网络安全的核心技术，在网络安全领域占有不可替代的重要地位。
第2章详细介绍了密码学的基本概念、对称密码学、数据加密标准DES、高级加密标准AES、RC4算法和基于对称密码的通信保密性等基础理论。
（3）公钥密码体制不仅用于加解密，而且可以广泛用于消息鉴别、数字签名和身份认证等服务，是密码学中一个开创性的成就。
公钥密码体制的最大优点是适应网络的开放性要求，密钥管理相对于对称密码体制要简单得多。
但是，公钥密码体制并不会取代对称密码体制，原因在于公钥密码体制算法相对复杂，加解密速度较慢。
实际应用中，公钥密码和对称密码经常结合起来使用，加解密使用对称密码技术，而密钥管理使用公钥密码技术。
第3章详细讨论了公钥密码体制原理、ElGamal公钥密码体制、密钥管理等基础理论。

<<计算机网络安全>>

内容概要

本书系统介绍了计算机网络安全知识和理论，内容包括计算机网络安全概述、对称密码学、高级加密标准、公钥密码学、消息鉴别、数字签名、身份认证、IP安全、web安全性、电子邮件安全、系统安全。

本书每章结尾附有习题和答案，便于读者理解所学内容。

本书可作为信息安全、计算机和通信等专业本科生和研究生的教科书，也可供从事相关专业的教学、科研和工程人员参考。

<<计算机网络安全>>

书籍目录

章节摘录

插图：攻击者攻击目标明确，针对网站和用户使用不同的攻击手段。
对政府网站主要采用篡改网页的攻击形式，对企业则采用有组织的分布式拒绝服务（DDOS）等攻击手段，对个人用户则通过窃取账号、密码等形式窃取用户个人财产，对金融机构则用网络钓鱼进行网络仿冒，在线盗取用户身份和密码。
在2008年中，病毒木马呈现爆发性增长，制作病毒木马门槛的降低和背后的高利益诱惑都是其主因。
2008年上半年，国家互联网应急中心（CNCERT）对常见的木马程序活动状况进行了抽样监测，发现我国大陆地区302526个IP地址的主机被植入木马。
包含恶意代码URL链接的垃圾邮件的数量有所增加，载有恶意软件（不仅仅是恶意代码的链接）的电子邮件数量也在不断增加。
针对DNS和域名转发服务器的攻击数量有明显增多的趋势。
新型网络应用的发展带来了新的安全问题和威胁。
当今社会，互联网已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用。
随着我国政府信息化基础建设的推进，信息公开程度的提升，网络和信息安全也已成为关系到国家安全、社会稳定的重要因素，社会各界都对网络安全提出了更高的要求，采取有效措施，建设安全、可靠、便捷的网络应用环境，维护国家网络信息安全，成为社会信息化进程中亟待解决的问题。
网络安全指网络系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，网络系统连续可靠正常地运行，网络服务不中断。
计算机网络是地理上分散的多台自主计算机互联的集合。
互联由各种各样的通信设备、通信链路、网络软件实现，而且必须遵循特定的网络协议。
因此，网络安全从其本质上讲就是网络上的信息安全。
为了保证网络上信息的安全，首先需要自主计算机系统的安全；其次需要互联的安全，即连接自主计算机的通信设备、通信链路、网络软件和通信协议的安全；最后需要各种网络服务和应用的安全。
网络安全的具体含义会随着利益相关方的变化而变化。
从一般用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时能够保持机密性、完整性和真实性，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯自身的利益。
从网络运行者和管理者角度说，他们希望对网络信息的访问受到保护和控制，避免出现非法使用、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。
安全保密部门希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。
从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

编辑推荐

《计算机网络安全》：理论与实践紧密结合，反映了计算机网络安全技，术的最新发展，强调计算机网络安全的基本原理和技术，注重计，算机网络安全技术的实际应用，适合学生循序渐进地学习。

<<计算机网络安全>>

版权说明