<<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

<<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。

<<计算机网络安全>>

书籍目录

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。

<<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。

<<计算机网络安全>>

版权说明