<<网络安全概论>>

图书基本信息

书名：<<网络安全概论>>

13位ISBN编号：9787121091001

10位ISBN编号：7121091003

出版时间：2009-7

出版时间：刘建伟、毛剑、 胡荣磊 电子工业出版社 (2009-07出版)

作者：刘建伟 等 著

页数：344

前言

信息化是世界经济和社会发展的必然趋势。
近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。
信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。
作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻陆、全局陆和战略陆的问题进行调查研究，提出政策建议和咨询意见。
在做这些工作的过程中，我们愈发认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一个紧迫需求，成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。
2006年5月，我国《2006－2010年国家信息化发展战略》公布，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。
为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版物等各种方式推动信息化知识的宣传、教育和培训工作。
2007年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。
编写该系列丛书的目的，是力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。
毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

<<网络安全概论>>

内容概要

《网络安全概论》介绍了网络安全的基本概念，较深入地讨论了网络边界安全、电子商务安全及通信网安全的理论与技术，内容基本上涵盖了网络安全理论与技术的各方面，其知识单元和知识点符合教育部信息安全类专业教学指导委员会制定的《信息安全类专业指导性专业规范》的要求。
《网络安全概论》力求概念清楚、语言精练。
在网络安全基本概念和理论介绍方面，力求深入浅出，尽可能将复杂的工作原理借助图表加以表述，以适应本科教学的特点。
特别是《网络安全概论》在每章的后面提供了很多填空题和思考题，便于进一步加深读者对课堂上所学知识的理解，并让读者深入思考一些有关网络安全的技术问题。
《网络安全概论》既可以作为高等学校信息安全、信息对抗、密码学、通信、计算机等专业高年级本科生和研究生的教材，也可以作为网络安全工程师、网络管理员和计算机用户的参考书或培训教材。

<<网络安全概论>>

书籍目录

章节摘录

插图：运行密钥建立协议可在两个或多个实体之间建立共享秘密，该共享秘密可用于数据加密，通常用做建立一次通信时的会话密钥。
下面主要讨论在两个实体之间建立共享秘密的密码协议。
密码协议可以采用单钥、双钥技术实现，有时也要借助可信第三方（TTP）的参与。
我们可以将密码协议扩展到建立多方共享密钥，如会议密钥建立，但随着参与方的增多，协议会变得很复杂。
在保密通信中，我们通常对每次会话都采用不同的密钥进行加密。
因为这个密钥只用于对某个特定的通信会话进行加密，所以被称为会话密钥。
会话密钥只在通信的持续时间内有效，当通信结束后，会话密钥会被清除。
如何将这些会话密钥分发到会话者的手中，是本节讨论的主要问题。
1.采用单钥体制的密钥建立协议密钥建立协议主要可分为密钥传输协议和密钥协商协议，前者是由一个实体把生成或收到的密钥安全传送给另一个实体，而后者是由双方（或多方）共同提供信息建立共享密钥，任何一方都不单独起决定作用。
其他协议，如密钥更新、密钥推导、密钥预分配、动态密钥建立协议等，都可在上述两种基本密钥建立协议的基础上进行演变而得出。
可信服务器（或可信第三方、认证服务器、密钥分配中心：KDC、密钥传递中心KTC、证书发行机构CA等）可以在初始化建立阶段或在线实时通信时，或者两种情况同时存在的情况下参与密钥分配。
这类协议假设网络用户Alice和Bob各自都与密钥分配中心：KDC（在协议中扮演Trent的角色）共享一个密钥。
这些密钥在协议开始之前必须已经分发到位。
协议描述如下：（1）Alice呼叫Trent，并请求得到与Bob通信的会话密钥：（2）Trent生成一个随机会话密钥，并做两次加密，一次采用Alice的密钥，另一次采用Bob的密钥，Ttent将两次加密的结果都发送给Alice。

<<网络安全概论>>

编辑推荐

《网络安全概论》由电子工业出版社出版。

版权说明