第一图书网, tushu007.com

<<网络安全协议理论与技术>>

图书基本信息

书名：<<网络安全协议理论与技术>>

13位ISBN编号：9787302193005

10位ISBN编号：7302193002

出版时间：2009-2

出版时间：清华大学出版社

作者：范明钰，王光卫　编著

页数：223

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

内容概要

本书从基本概念入手，通过Internet协议的实际例子，建立网络协议的概念，分析了Internet协议不安全的原因，介绍了安全协议的密码学基础，分析了安全协议与密码学的关系，介绍了利用不同的密码算法建立安全信道。
从第4章开始，介绍基本的安全协议、抗攻击的安全协议和实际使用的安全协议。
附录中介绍了最新的几类密码算法。
每章都附有重点和难点分析，并附有习题与思考题。
全书共分为三个部分：第一部分介绍基本概念和Internet中的协议（第1章和第2章）。
第二部分介绍安全协议，分为三个内容、安全协议的密码学基础（第3章）、基本安全协议（第4章）和抗攻击的安全协议（第5章）。
第三部分介绍实际使用的安全协议（第6章）。
这三个部分基本上是关联的，既可以从概念入手讲解，也可以先从实际例子开始最后得到理性的知识。
本书可供工科类计算机、电子信息、通信等相关学科的本科学生和研究生使用。

书籍目录

第1章　基本概念　1.1　网络基础及网络协议的概念　1.1.1　网络的构成和分类　1.1.2　网络的发展　1.2　网络安全的概念　1.2.1　网络安全的含义　1.2.2　不同环境和应用中的网络安全　1.2.3　网络安全的重要性　1.2.4　关于安全的权衡　1.3　网络中的协议　1.3.1　基本概念　1.3.2　网络协议的定义　1.3.3　协议的目的　1.3.4　协议中的角色　1.3.5　协议的分类　1.4　网络协议面临的威胁　1.5　本章重点和难点　习题与思考题第2章　Internet的协议　2.1　Internet协议的基本构架　2.1.1　协议堆栈　2.1.2　数据流分析　2.1.3　网络层和传送层　2.1.4　定址　2.1.5　路由　2.2　导致Internet不安全的原因　2.3　Internet中与安全相关的协议　2.3.1　实施安全保护的层次　2.3.2　应用层　2.3.3　传送层　2.3.4　网络层　2.3.5　数据链路层　2.4　网络层的安全协议IPSec　2.4.1　IPSec的体系结构　2.4.2　安全关联和安全策略　2.4.3　IPSec协议的运行模式　2.4.4　AH协议　2.4.5　ESP协议　2.4.6　Internet密钥交换协议　2.5　本章重点和难点　习题与思考题第3章　安全协议的密码学基础　3.1　安全协议与密码学的关系　3.2　密码算法　3.2.1　对称密码算法　3.2.2　非对称密码算法　3.2.3　Hash算法　3.2.4　一次一密乱码本　3.3　利用密码算法建立安全通信信道　3.3.1　对称密码技术　3.3.2　公开密钥密码技术　3.3.3　混合密码系统　3.4　不使用密码算法的安全协议的例子　3.5　Hash算法的使用——数字签名　3.5.1　算法和术语　3.5.2　使用对称密码系统和仲裁者的文件签名　3.5.3　数字签名树　3.5.4　使用公钥密码对文件签名　3.5.5　文件签名和时间标记　3.5.6　用公钥密码和单向Hash算法对文件签名　3.5.7　多重签名方案　3.5.8　抗抵赖的数字签名　3.5.9　数字签名的国际应用　3.6　本章重点和难点　习题与思考题第4章　基本安全协议第5章　抗攻击的安全协议第6章　实际使用的安全协议附录参考文献

章节摘录

第1章　基本概念1.1 网络基础及网络协议的概念简单地说，网络是由两台以上计算机借助于协议连在一起组成的“ 计算机群 ”，再加上相应“ 通信设备 ”组成的综合系统。
早期的计算机应用模式是单机，其发展过程有小型机、中型机、大型机。
单台计算机能干很多事情。
虽然计算机的速度越来越快、性能越来越高、容量越来越大，但还是存在一些美中不足。
比如办公室为每个人都配备了一台最新式计算机，但是打印机的配备却成了问题。
如果只为一台或者几台计算机配备打印机，那些没有配备打印机的人打印时就需要把文件用磁盘复制到有打印机的计算机上去打印，不仅麻烦，而且也耽误别人的时间。
另一方面，如果给所有计算机都配备打印机，它们多数情况下是处于闲置状态，很明显这是一种浪费。
如果只给一台或几台计算机配备打印机，而其他所有计算机都可以利用这些打印机，并且相互之间不影响工作，这就是资源共享。
可以在网络上共享的资源除了打印机之外，还有硬盘、光盘、绘图仪、扫描仪以及各类软件、文本和各种信息资源等。
在网络中共享资源既节省了大量的投资和开支，又便于集中管理。
利用网络可以进行信息交换和信息的集中与分散处理，比如说一家公司，有生产部、仓储部、市场部、财务部等很多部门和分公司。
这些部门和分公司在地理位置上并不在一起。
但是作为一个现代化的大公司，各个业务部门需要随时知道其他部门的各种数据：分散的销售数据需要及时集中起来配合仓储部的库存和生产部的生产，分散的财务数据也需要随时送到财务部集中处理以配合公司的整体行动。
诸如此类，称为信息交换和信息的集中与分散处理。
这些都需要依托网络才能做到。
计算机网络并不是随着计算机的出现而出现的，而是随着社会对资源共享和信息交换与及时传递的迫切需要而发展起来的。
它是现代计算机技术和通信技术密切结合的产物。
说得准确一些，计算机网络就是利用通信设备和通信线路，把位于不同地点的计算机等设备相互联起来，用相应的协议软件实现资源共享和信息交换的系统。

编辑推荐

《网络安全协议理论与技术》可供工科类计算机、电子信息、通信等相关学科的本科学生和研究生使用。

第一图书网, tushu007.com

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