第一图书网, tushu007.com

<<信息安全技术>>

图书基本信息

书名：<<信息安全技术>>

13位ISBN编号：9787560621951

10位ISBN编号：7560621953

出版时间：2009-2

出版时间：西安电子科技大学出版社

作者：赵泽茂,吕秋云,朱芳

页数：340

字数：517000

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

全书共分15章，内容包括信息安全概述、信息保密技术、信息隐藏技术、消息认证技术、密钥管理技术、数字签名技术、物理安全、操作系统安全、网络安全协议、应用层安全技术、网络攻击技术、网络防御技术、计算机病毒、信息安全法律与法规、信息安全解决方案等。
?
本书可作为计算机、通信、电子工程、信息对抗、信息管理、信息安全及其他电子信息类相关专业的本科生教材，也可作为高等学校及各类培训机构相关课程的教材或教学参考书，还可供从事信息安全、信息处理、计算机、电子商务等领域工作的科研人员和工程技术人员参考。

书籍目录

第1章 信息安全概述
1.1 信息安全现状
1.1.1 信息安全的威胁
1.1.2 信息安全涉及的问题
1.1.3 信息安全的困惑
1.2 信息安全需求
1.2.1 信息安全的含义
1.2.2 基本服务需求
1.3 网络不安全的根本原因
1.3.1 系统漏洞
1.3.2 协议的开放性
1.3.3 人为因素
1.4 信息安全体系结构
1.4.1 OSI安全体系结构
1.4.2 TCP／IP安全体系结构
1.4.3 信息安全保障体系
小结
习题
第2章 信息保密技术
2.1 密码学的发展简史
2.2 密码学中的基本术语
2.3 古典密码
2.4 对称密码体制
2.4.1 序列密码
2.4.2 分组密码
2.4.3 数据加密标准——DES
2.5 非对称密码体制
2.5.1 RSA密码算法
2.5.2 Diffie—Hellman密钥交换算法
2.5.3 ElGamal加密算法
2.6 密码学的应用
2.6.1 密码应用模式
2.6.2 加密方式
2.6.3 PGP软件的应用
小结
习题
第3章 信息隐藏技术
3.1 信息隐藏的发展历史
3.1.1 传统的信息隐藏技术
……
第4章 消息认证技术
第5章 密钥管理技术
第6章 数字签名技术
第7章 物理安全
第8章 操作系统安全

第一图书网, tushu007.com

第9章 网络安全协议
第10章 应用层安全技术
第11章 网络攻击技术
第12章 网络防御技术
第13章 计算机病毒
第14章 信息安全法律与法规
第15章 信息安全解决方案
附录 实验
部分习题参考答案
参考文献

章节摘录

插图：（4）信息发送者对发送过的信息或完成的某种操作是承认的，这就是用户对信息发送者提出的不可否认的要求。
从网络运行和管理者的角度来讲，他们希望本地信息网正常运行，正常提供服务，不受网外攻击，未出现计算机病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁。
从安全保密部门的角度来讲，他们希望对非法的、有害的、涉及国家安全或商业机密的信息进行过滤和防堵，避免通过网络泄露关于国家安全或商业机密的信息，避免对社会造成危害，对企业造成经济损失。
从社会教育和意识形态的角度来讲，我们应避免不健康内容的传播，正确引导积极向上的网络文化。
2.信息安全的狭义解释信息安全在不同的应用环境下有不同的解释。
针对网络中的一个运行系统而言，信息安全就是指信息处理和传输的安全。
它包括硬件系统的安全可靠运行、操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等.狭义的信息安全，就是指信息内容的安全，包括信息的保密性、真实性和完整性。
3.信息安全的广义解释广义的信息安全是指网络系统的硬件、软件及其系统中的信息受到保护。
它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改和泄露。
网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全，可见，这与其所保护的对象有关。
1.2.2 基本服务需求1.保密性保密性是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用。
这些信息不仅包括国家机密，也包括企业和社会团体的商业机密和工作机密，还包括个人信息。
人们在应用网络时很自然地要求网络能提供保密性服务，而被保密的信息既包括在网络中传输的信息，也包括存储在计算机系统中的信息。
就像电话可以被窃听一样，网络传输信息也可以被窃听，解决的办法就是对传输信息进行加密处理。
存储信息的机密性主要通过访问控制来实现，不同用户对不同数据拥有不同的权限。
2.完整性完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
数据的完整性的目的是保证计算机系统上的数据和信息处于一种完整和未受损害的状态，这就是说数据不会因为有意或无意的事件而被改变或丢失。
除了数据本身不能被破坏外，数据的完整性还要求数据的来源具有正确性和可信性，也就是说需要首先验证数据是真实可信的，然后再验证数据是否被破坏。

编辑推荐

《信息安全技术》系统介绍了信息安全相关技术，内容包括信息安全概述、信息保密技术、信息隐藏技术、消息认证技术、密钥管理技术、数字签名技术等。

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