第一图书网, tushu007.com

<<信息安全导论>>

图书基本信息

书名：<<信息安全导论>>

13位ISBN编号：9787111362722

10位ISBN编号：7111362721

出版时间：2012-1

出版时间：机械工业出版社

作者：何泾沙　主编

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

《信息安全导论》作为一本信息安全方面的导论书籍，结合信息安全领域的前沿研究，借鉴和引用国内外的相关文献资料，较全面、系统地介绍了信息安全的基本概论和知识。
本书介绍了信息安全所涉及的基本概念、所依赖的模型和理论基础以及所使用的信息保护方法，从数据加密保护及密钥管理、数字签名、身份识别及认证、访问控制、信息流安全分析及安全保障方法等方面全面介绍了信息安全的相关技术和手段，最后以网络安全为主线介绍了信息安全在网络环境中所面临的挑战和应对措施以及当前信息安全方法和技术的研究和发展现状。
通过阅读本书，读者能够对计算机系统和网络环境中的信息安全问题和基本解决思路及方法有一个初步的、较全面的理解和掌握，为读者今后在信息安全领域进行深入研究和进一步学习打下良好的基础。

《信息安全导论》可作为高等院校信息安全、计算机科学与技术、软件工程及相关信息类专业“信息安全概论”或“信息安全导论”课程的教材，同时也适合希望了解信息安全领域中基本知识的其他读者阅读。

第一图书网, tushu007.com

书籍目录

编委会
丛书序
前言
教学及阅读建议
第1章　绪论
1.1　信息安全概述
1.2　信息安全面临的威胁
1.3　信息安全策略和机制
1.3.1　信息安全管理体系
1.3.2　信息安全等级保护
1.3.3　信息安全风险评估
1.3.4　信息安全与法律
1.4　国内外信息安全现状和特点
1.5　本章小结
习题
第2章　信息安全模型与策略
2.1　访问控制矩阵模型
2.1.1　保护状态
2.1.2　模型描述
2.1.3　保护状态转换
2.2　安全策略
2.2.1　安全策略的内涵及职能
2.2.2　安全策略的类型
2.2.3　访问控制的类型
2.3　保密性模型与策略
2.3.1　保密性策略的目标
2.3.2　bell-lapadula模型
2.3.3　bell-lapadula模型的拓展
2.3.4　bell-lapadula模型的局限性
2.4　完整性模型与策略
2.4.1　完整性策略的目标
2.4.2　biba完整性模型
2.4.3　lipner完整性模型
2.4.4　clark-wilson完整性模型
2.5　混合型模型与策略
2.5.1　混合型策略的目标
2.5.2　chinese wall模型
2.5.3　医疗信息系统安全模型
2.5.4　基于创建者的访问控制模型
2.5.5　基于角色的访问控制模型
2.6　本章小结
习题
第3章　密码学原理及密钥管理
3.1　密码学基础
3.1.1　密码学发展简史

3.1.2　密码学研究目标
3.1.3　密码体制
3.1.4　密码体制安全性
3.1.5　密码分析
3.2　加密方法及技术
3.2.1　基于共享密钥的加密方法及技术
3.2.2　基于公钥的加密方法及技术
3.3　密钥管理方法及技术
3.3.1　基于共享密钥系统的密钥管理方法及技术
3.3.2　基于公钥系统的密钥管理方法及技术
3.4　本章小结
习题
第4章　数字签名
4.1　数字签名概述
4.1.1　数字签名的概念
4.1.2　数字签名的功能与性质
4.1.3　数字签名与手写签名
4.1.4　对数字签名的攻击
4.2　数字签名体制
4.2.1　数字签名的过程
4.2.2　签名技术的要求
4.2.3　数字签名的分类
4.3　直接方式的数字签名技术
4.4　具有仲裁方式的数字签名技术
4.4.1　仲裁方式的一般实施方案
4.4.2　基于传统密钥明文可见的仲裁方案
4.4.3　基于传统密钥明文不可见的仲裁方案
4.4.4　基于公钥的仲裁方案
4.5　基于公钥的数字签名技术
4.5.1　rsa数字签名
4.5.2　rabin数字签名
4.5.3　elgamal数字签名
4.5.4　dsa数字签名
4.6　其他数字签名技术
4.6.1　盲签名
4.6.2　不可否认签名
4.6.3　批量签名
4.6.4　群签名
4.6.5　代理签名
4.6.6　同时签约
4.7　本章小结
习题
第5章　认证及身份验证技术
5.1　身份与认证
5.1.1　身份及身份鉴别
5.1.2　认证
5.2　身份验证技术

5.2.1 口令
5.2.2 质询-应答协议
5.2.3 利用信物的身份认证
5.2.4 生物认证
5.3 kerberos认证系统
5.4 本章小结
习题
第6章 访问控制技术及实现
6.1 访问控制和安全机制的设计原则
6.1.1 访问控制技术
6.1.2 安全机制的设计原则
6.2 访问控制列表
6.2.1 访问控制矩阵与访问控制列表
6.2.2 实例分析：windows nt和unix访问控制列表
6.3 能力表
6.3.1 能力表的概念及实例
6.3.2 基于能力表的自主访问控制
6.3.3 能力表的保护和权限的撤销
6.3.4 能力表和访问控制列表的比较
6.4 锁与钥匙
6.4.1 锁与钥匙的密码学实现
6.4.2 机密共享问题
6.5 基于环的访问控制方法
6.6 传播性访问控制列表
6.7 本章小结
习题
第7章 信息流安全分析
7.1 基础与背景
7.1.1 信息流控制策略
7.1.2 信息流模型与机制
7.2 基于编译器机制的信息流检测
7.3 基于执行机制的信息流检测
7.3.1 fenton的数据标记机
7.3.2 动态安全检查
7.4 信息流控制实例
7.5 隐信道
7.5.1 隐信道概念
7.5.2 隐信道分类
7.5.3 隐信道分析
7.6 本章小结
习题
第8章 安全保障
8.1 保障模型和方法
8.1.1 安全保障和信任
8.1.2 建造安全可信的系统
8.1.3 形式化方法
8.2 审计

8.2.1　定义
8.2.2　剖析审计系统
8.2.3　设计审计系统
8.2.4　事后设计
8.2.5　审计机制
8.2.6　审计文件系统实例
8.2.7　审计信息浏览
8.3　系统评估
8.3.1　可信计算机系统评估标准简介
8.3.2　国际安全标准简介
8.3.3　我国安全标准简介
8.4　本章小结
习题
第9章　网络安全
9.1　恶意攻击
9.1.1　概述
9.1.2　特洛伊木马
9.1.3　计算机病毒
9.1.4　计算机蠕虫
9.1.5　其他形式的恶意代码
9.1.6　恶意代码分析与防御
9.2　网络安全漏洞
9.2.1　概述
9.2.2　系统漏洞分类
9.2.3　系统漏洞分析
9.3　入侵检测
9.3.1　原理
9.3.2　基本的入侵检测
9.3.3　入侵检测模型
9.3.4　入侵检测体系结构
9.3.5　入侵检测系统的分类
9.3.6　入侵响应
9.3.7　入侵检测技术发展方向
9.4　p2dr安全模型
9.5　网络安全案例
9.5.1　常用技术
9.5.2　案例概述
9.5.3　策略开发
9.5.4　网络组织
9.5.5　可用性和泛洪攻击
9.6　本章小结
习题
参考文献

章节摘录

版权页：插图：1.泄露嗅探，即对信息的非法拦截，是某种形式的信息泄露。
嗅探是被动的，其目的是窃听消息或者仅仅浏览信息。
被动搭线窃听就是一种监视网络的嗅探形式，它把未经批准的装置（如计算机终端）连接到通信线路上，通过生成错误信息或控制信号，或者通过改换合法用户的通信方式以获取对数据的访问。
保密性可以对抗这种威胁。
2.欺骗篡改，即对信息的非授权改变。
篡改是主动的，共目的可能是欺骗。
主动搭线窃听就是篡改的一种形式，在窃听过程中，传输于网络中的数据会被篡改。
中间人攻击就是一种主动搭线窃听的例子。
入侵者从发送者那里读取消息，再将修改过的消息发往接收者，希望接收者和发送者不会发现中间人的存在。
完整性能对抗这种威胁。
伪装，即一个恶意实体假冒为另一个友好实体，诱使用户相信与之通信的就是被冒充的友好实体本身，它是兼有欺骗和篡夺的一种手段。
网络钓鱼就是伪装的一种形式，在钓鱼过程中，攻击者将用户引诱到一个精心设计的与目标网站非常相似的钓鱼网站上，并获取用户在此网站上输入的个人敏感信息而不让用户察觉。
网络钓鱼的危害已经超过传统的病毒和木马，成为威胁网民利益的第一杀手。
钓鱼网站主要以虚假中奖、虚假购物和虚假广告等方式存在，81%是各种各样的中奖骗局，尤其以“腾讯QQ周年庆典抽奖”、“非常6+1抽奖”骗局最为普遍。
据估计，网络钓鱼给社会带来的间接损失可能超过200亿元。
完整性能对抗这种威胁。

编辑推荐

《信息安全导论》结合作者多年在国内外数家著名IT公司以及高等院校从事信息安全技术研发和课程教学的丰富经验编写而成，采用理论与实践相结合的方式，在知识领域、知识单元和知识点三个层次上构建整个知识体系.书中除了介绍信息安全的基本概念、理论、方法和过程外，还通过实际案例讲述信息安全在项目中的应用和体现，另外《信息安全导论》还配有适量的习题，可以作为学习和教学的辅助资料。
《信息安全导论》特点：实用性：根据学习与参考的需要，全面介绍信息安全的基础知识及应用，并给出相应的习题，以加强对理论知识的理解与掌握。
可读性：按照基础理论和知识、相关技术和方法、小结的顺序来组织内容，逻辑性强，层次分明，叙述准确而精炼，便于学习和理解。
时效性密切关注国内外信息安全领域的研究动态，使《信息安全导论》在内容上及时反映信息安全领域的新发展和新应用。
完整性：以具体的网络安全案例贯穿相关内容，使读者在阅读和学习的过程中体会和理解信息安全的基本知识和相关技术的应用。

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