<<信息安全原理及应用>>

图书基本信息

书名：<<信息安全原理及应用>>

13位ISBN编号：9787302254188

10位ISBN编号：7302254184

出版时间：2012-1

出版时间：清华大学出版社

作者：熊平 编

页数：319

字数：528000

<<信息安全原理及应用>>

内容概要

本书共分为13章，分别介绍信息安全的基本概念、目标和研究内容；密码学的基本概念；对称密码体制和公钥密码体制；密码学理论的应用机制；访问控制技术；网络攻击技术和恶意代码分析；网络安全防御系统；网络层、传输层及应用层的安全协议；评估信息系统安全的国内外标准；附录为8个信息安全实验。

《信息安全原理及应用（第2版）》可作为信息安全、计算机应用、信息管理等相关专业本科生或研究生的教材和参考书，也可供从事安全技术和管理工作人员参考。

<<信息安全原理及应用>>

书籍目录

第1章 信息安全概述
1.1 信息安全的概念
1.2 信息安全的发展历史
1.3 信息安全的目标
1.3.1 安全性攻击
1.3.2 信息安全的目标
1.4 信息安全的研究内容
1.4.1 信息安全基础研究
1.4.2 信息安全应用研究
1.4.3 信息安全管理研究
第2章 密码学基础
2.1 密码学的发展历史
2.2 密码学的基本概念
2.3 密码系统的分类
2.4 密码分析
2.4.1 密码分析学
2.4.2 穷举攻击
2.5 经典密码学
2.5.1 代换密码
2.5.2 置换技术
2.5.3 转轮机
2.5.4 隐蔽通道和隐写术
第3章 对称密码体制
3.1 分组密码
3.2 数据加密标准
3.2.1 数据加密标准简介
3.2.2 DES加密解密原理
3.2.3 DES的安全性
3.2.4 多重DES
3.3 高级加密标准AES
3.3.1 AES概述
3.3.2 AES加密数学基础
3.3.3 AES加密原理
3.3.4 AES的解密变换
3.3.5 AES加密算法性能分析
3.4 序列密码
3.4.1 序列密码的原理
3.4.2 RC4
3.5 其他对称加密算法
第4章 公钥密码体制
4.1 公钥密码体制的产生
4.2 数论基础
4.2.1 基本概念
4.2.2 欧几里得算法
4.2.3 乘法逆元

4.2.4 费尔马小定理
4.2.5 欧拉函数和欧拉定理
4.2.6 离散对数
4.3 公钥密码体制的基本原理
4.3.1 公钥密码体制的基本构成
4.3.2 加密解密协议
4.3.3 公钥密码应满足的要求
4.4 RSA公钥密码体制
4.4.1 RSA算法
4.4.2 RSA算法在计算上的可行性分析
4.4.3 RSA的安全性
4.5 其他公钥密码算法
4.5.1 ElGamal密码
4.5.2 椭圆曲线密码体制
第5章 消息认证
5.1 消息认证基本概念
5.2 消息加密认证
5.3 消息认证码
5.3.1 消息认证码的基本用法
5.3.2 消息认证码的安全性
5.3.3 基于DES的消息认证码
5.4 Hash函数
5.4.1 基本概念
5.4.2 认证方法
5.4.3 常用Hash算法
5.4.4 对Hash函数的攻击
第6章 身份认证与数字签名
6.1 身份认证
6.1.1 身份认证的物理基础
6.1.2 身份认证方式
6.1.3 Kerberos协议
6.1.4 零知识证明
6.2 数字签名
6.2.1 数字签名原理
6.2.2 数字签名算法
第7章 密钥管理
7.1 对称密码体制的密钥管理
7.1.1 密钥分级
7.1.2 密钥生成
7.1.3 密钥的存储与备份
7.1.4 密钥分配
7.1.5 密钥的更新
7.1.6 密钥的终止和销毁
7.2 公钥密码体制的密钥管理
7.2.1 公钥的分配
7.2.2 数字证书
7.2.3 X.509证书

7.2.4 公钥基础设施
第8章 访问控制
8.1 访问控制概述
8.2 访问控制策略
8.2.1 自主访问控制
8.2.2 强制访问控制
8.2.3 基于角色的访问控制
8.2.4 基于任务的访问控制
8.2.5 基于对象的访问控制
8.3 网络访问控制的应用
8.3.1 MAC地址过滤
8.3.2 VLAN隔离
8.3.3 ACL访问控制列表
8.3.4 防火墙访问控制
第9章 网络攻击技术
9.1 侦查
9.2 扫描
9.2.1 端口扫描
9.2.2 漏洞扫描
9.2.3 实用扫描器简介
9.3 获取访问权限
9.3.1 缓冲区溢出
9.3.2 SQL注入攻击
9.4 保持访问权限
9.5 消除入侵痕迹
9.6 拒绝服务攻击
第10章 恶意代码分析
10.1 病毒
10.1.1 感染
10.1.2 传播机制
10.1.3 防御病毒
10.2 蠕虫
10.3 恶意移动代码
10.4 后门
10.5 特洛伊木马
10.6 RootKit
第11章 网络安全防御系统
11.1 防火墙系统
11.1.1 防火墙的定义
11.1.2 防火墙的分类
11.1.3 包过滤防火墙
11.1.4 状态防火墙
11.1.5 应用网关防火墙
11.1.6 混合防火墙与防火墙系统
11.1.7 防火墙的体系结构
11.2 入侵检测系统
11.2.1 入侵检测系统概述

11.2.2 入侵检测系统分类
11.2.3 入侵检测方法
11.2.4 网络入侵检测系统Snort简介
11.2.5 入侵检测的局限性与发展方向
11.3 入侵防御系统
11.3.1 入侵防御系统概述
11.3.2 入侵防御系统的原理
11.3.3 IPS的分类
11.3.4 IPS的局限性
11.4 统一威胁管理UTM
11.4.1 UTM概述
11.4.2 UTM技术原理
11.4.3 UTM的优势与局限性
第12章 安全协议
12.1 安全协议概述
12.1.1 安全协议基本概念
12.1.2 TCP/IP安全分析
12.1.3 TCP/IP安全架构
12.2 IPSec协议
12.2.1 基本概念和术语
12.2.2 IPSec组成
12.2.3 IPSec的工作模式
12.2.4 IPSec的应用
12.3 SSL协议
12.3.1 SSL协议概述
12.3.2 SSL协议的分层结构
12.3.3 SSL握手协议
12.3.4 SSL记录协议
12.3.5 SSL协议安全性分析
12.4 安全电子交易协议
12.4.1 SET协议概述
12.4.2 SET交易的参与者
12.4.3 双重签名
12.4.4 SET的交易流程
12.4.5 SET协议的安全性分析
第13章 安全评价标准
13.1 可信计算机系统评价标准
13.1.1 TCSEC的主要概念
13.1.2 计算机系统的安全等级
13.2 通用评估准则
13.2.1 CC的主要用户
13.2.2 CC的组成
13.2.3 评估保证级别EAL
13.2.4 CC的特点
13.3 我国信息系统安全评价标准
13.3.1 所涉及的术语
13.3.2 等级的划分及各等级的要求

13.3.3 对标准的分析
附录A 信息安全实验
A1 三重DES加密软件的开发
A2 PGP软件的使用
A3 配置访问控制列表
A4 网络侦听及协议分析
A5 VRRP协议及其配置
A6 Windows XP防火墙的配置
A7 入侵检测系统Snort的使用
A8 信息系统安全保护等级定级
参考文献

章节摘录

版权页： 插图： 1.3.1安全性攻击 为了获取有用的信息或达到某种目的，攻击者会采取各种方法对信息系统进行攻击。
这些攻击方法分为两类：被动攻击和主动攻击。
其中，被动攻击试图了解或利用通信系统的信息但不影响系统资源，而主动攻击则试图改变系统资源或影响系统运作。
1.被动攻击 被动攻击指攻击者在未被授权的情况下，非法获取信息或数据文件，但不对数据信息做任何修改，通常包括监听未受保护的通信、流量分析、解密弱加密的数据流、获得认证信息等。
被动攻击的特性是对传输进行窃听和监测，攻击者的目标是获得传输的信息。
常用的被动攻击手段如下所述。
（1）搭线监听：搭线监听是将导线搭到无人值守的网络传输线路上进行监听。
只要所搭的监听设备不影响网络负载，通常不易被发觉。
然后通过解调和正确的协议分析，就可以掌握通信的全部内容。
（2）无线截获：通过高灵敏接收装置接收网络站点或网络连接设备辐射的电磁波，然后对电磁信号进行分析，可以恢复数据信号进而获得网络传输的信息。
对于无线网络通信，无线截获与搭线监听有同样的效果。
（3）其他截获：用程序和病毒截获信息是计算机技术发展的新型手段，在通信设备或主机中种植木马或施放病毒程序后，这些程序会将有用的信息通过某种方式远程发送出来。
（4）流量分析：假设通过某种手段（如加密）使得攻击者从截获的信息中无法得到消息的真实内容。
攻击者还可以通过观察这些数据的模式，分析出通信双方的位置、通信的次数及消息的长度等信息，而这些信息可能对通信双方来说也是不希望被攻击者得知的，这种攻击手段称为流量分析。
被动攻击由于不涉及对数据的更改，所以很难察觉。
然而通过加密的手段阻止这种攻击却是可行的。
因此对付被动攻击的重点是预防，而不是检测。
2.主动攻击 主动攻击包括对数据流进行篡改或伪造，可分为4类。
（1）伪装：指某实体假冒别的实体，以获取合法用户的被授予的权利。
（2）重放：指攻击者对截获的合法数据进行复制，然后出于非法目的再次生成，并在非授权的情况下进行传输。
（3）消息篡改：指对一个合法消息的某些部分进行修改、删除，或延迟消息的传输、改变消息的顺序，以产生混淆是非的效果。
（4）拒绝服务：阻止或禁止信息系统正常的使用。
它的主要形式是破坏某实体网络或信息系统，使得被攻击目标资源耗尽或降低其性能。
主动攻击的特点与被动攻击恰好相反。
被动攻击虽然难以检测，但可采取相应措施有效地防止，而要绝对防止主动攻击是十分困难的，因为需要保护的范围太广。
因此，对付主动攻击的重点在于检测并从攻击造成的破坏中及时地恢复。

编辑推荐

《重点大学信息安全专业规划系列教材:信息安全原理及应用(第2版)》实验教学是信息安全基础教学中不可缺少的内容，但目前的信息安全基础教材要么没有实验内容，要么有实验内容但对实验环境要求较高，在实际教学中没有可操作性。
因此，《重点大学信息安全专业规划系列教材:信息安全原理及应用(第2版)》在内容编排上，力求理论与实践相结合，包含了密码学基础理论、密码学应用机制、实用安全技术及相关实验内容，使读者能够更清晰地从信息安全体系的层面掌握信息安全的基础理论和应用技术。

<<信息安全原理及应用>>

版权说明