

<<信息系统安全理论与技术>>

图书基本信息

书名：<<信息系统安全理论与技术>>

13位ISBN编号：9787040233490

10位ISBN编号：7040233495

出版时间：2008-3

出版范围：高等教育

作者：方勇

页数：371

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>

<<信息系统安全理论与技术>>

内容概要

《高等学校信息安全系列教材：信息系统安全理论与技术》通过对信息系统安全的五大安全服务和多种实现机制给出比较完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

书籍目录

第1章 绪论 1.1 信息系统概述 1.1.1 信息系统的定义 1.1.2 信患系统的发展过程 1.2 信息系统安全 1.2.1 基本概念 1.2.2 信息保密与信息系统安全 1.3 影响信息系统安全的因素 1.3.1 信患系统自身的安全脆弱性 1.3.2 对信息系统安全的威胁 1.4 信息系统的安全策略 1.4.1 安全策略的基本原则 1.4.2 信患系统安全的工程原则 1.4.3 典型信息系统的安全需求分析 1.4.4 个人上网的安全需求分析 1.5 信息系统的风险和安全需求 1.5.1 信息系统的安全目标 1.5.2 信息系统安全的构成要素 1.6 信息系统安全保护等级划分准则 1.6.1 第一级——用户自主保护级 1.6.2 第二级——系统审计保护级 1.6.3 第三级——安全标记保护级 1.6.4 第四级——结构化保护级 1.6.5 第五级——访问验证保护级 本章小结 习题 第2章 信息系统安全体系 2.1 OSI 开放系统互连安全体系结构 2.1.1 安全体系的安全服务 2.1.2 安全体系的安全机制 2.2 TCP/IP安全体系 2.2.1 Internet网络体系结构 2.2.2 Internet全体系结构 2.3 开放互连系统的安全管理 2.3.1 安全管理的概念 2.3.2 开放系统互连的安全管理 本章小结 习题 第3章 信息安全技术原理 3.1 密码技术 3.1.1 概述 3.1.2 密码技术原理 3.1.3 密码算法 3.2 访问控制技术 3.2.1 概述 3.2.2 访问控制技术原理 3.2.3 网络访问控制组件的分布 3.2.4 访问控制信息的管理 3.3 机密性保护技术 3.3.1 概述 3.3.2 机密性保护技术的机制 3.4 完整性保护技术 3.4.1 概述 3.4.2 完整性机制的分类描述 3.5 鉴别技术 3.5.1 概述 3.5.2 鉴别技术原理 3.5.3 非密码鉴别机制 3.5.4 基于密码的鉴别机制 3.6 数字签名技术 3.6.1 概述 3.6.2 带附录的签名技术 3.6.3 带消息恢复的数字签名技术 3.7 抗抵赖技术 3.7.1 概述 3.7.2 抗抵赖技术的原理 3.7.3 抗抵赖技术面临的威胁 3.8 安全审计和报警机制 3.8.1 一般概念 3.8.2 安全报警报告功能 3.8.3 安全审计跟踪功能 3.9 公证技术 3.10 普遍安全技术 3.10.1 可信安全技术 3.10.2 安全标记技术 3.10.3 事件检测技术 3.10.4 安全恢复技术 3.10.5 路由选择技术 本章小结 习题 第4章 信息系统风险评估 4.1 概述 4.2 风险评估的概念 4.2.1 风险评估的定义 4.2.2 风险评估要解决的问题 4.2.3 风险评估的原则 4.3 风险评估的意义 4.4 风险评估的目的 4.5 风险评估的发展历程 4.5.1 国际风险评估的发展历程 4.5.2 我国的风险评估工作 4.6 风险评估要素及其关系 4.6.1 风险评估要素 4.6.2 风险评估要素关系模型 4.6.3 风险评估要素之间作用关系的形式化描述 4.7 风险评估指标体系 4.7.1 风险与安全事件 4.7.2 安全事件的影响因素 4.7.3 风险的确认 4.7.4 风险影响因素的特点 4.8 风险评估过程 4.8.1 业务需求与安全目标 4.8.2 资源分布 4.8.3 脆弱性分析 4.8.4 威胁源分析 4.8.5 威胁行为分析 4.8.6 风险分析 4.8.7 风险评估 4.8.8 安全需求导出 4.8.9 安全措施需求导出 4.8.10 实际安全措施与安全措施需求符合度检查 4.8.11 残留风险估计 4.9 风险评估与信息系统的生命周期 4.10 风险评估方法与工具 4.11 信息系统风险评估案例 本章小结 习题 第5章 个人计算机安全配置和管理 5.1 系统安装 5.1.1 选择操作系统 5.1.2 硬盘分区 5.1.3 系统补丁 5.2 系统用户管理和登录 5.2.1 系统用户账号 5.2.2 加强密码安全 5.2.3 系统登录控制 5.3 系统安全配置 5.3.1 系统服务管理 5.3.2 网络端口管理 5.3.3 网络共享控制 5.3.4 审计策略 5.3.5 本地安全策略 5.4 病毒防护 5.4.1 计算机病毒的定义 5.4.2 计算机病毒的命名规则 5.4.3 发现计算机病毒 5.4.4 清除计算机病毒 5.4.5 常用防护命令和工具介绍 5.4.6 流氓软件的清除 本章小结 习题 第6章 防火墙技术 6.1 基本概念 6.2 防火墙的基本类型 6.2.1 包过滤 6.2.2 应用网关 6.2.3 电路网关 6.2.4 混合型防火墙 6.3 防火墙的配置形式 6.3.1 包过滤路由器防火墙 6.3.2 双穴机网关防火墙 6.3.3 主机过滤防火墙 6.3.4 子网过滤防火墙 6.3.5 跨越公共网络的基于VPN的内联网防火墙系统 6.4 防火墙的局限性 6.5 防火墙的应用示例 6.5.1 主要特性 6.5.2 典型应用配置实例 本章小结 习题 第7章 漏洞检测技术 7.1 入侵攻击可利用的系统漏洞类型 7.1.1 网络传输和协议的漏洞 7.1.2 系统的漏洞 7.1.3 管理的漏洞 7.2 漏洞检测技术分类 7.3 漏洞检测的特点 7.4 漏洞检测系统的设计实例 7.4.1 设计目标 7.4.2 系统组成 7.4.3 外部扫描模块体系结构 7.4.4 内部扫描模块体系结构 7.4.5 系统工作过程 本章小结 习题 第8章 入侵检测预警技术 8.1 基本概念 8.2 针对TCP/IP协议安全缺陷的网络攻击 8.2.1 使用IP欺骗的TCP序列号攻击 8.2.2 利用源路径选项的安全漏洞进行攻击 8.2.3 针对ICMP报文的攻击 8.2.4 利用路由信息协议(RIP)的安全漏洞进行攻击 8.2.5 利用IP分组、重组算法的安全漏洞进行攻击 8.2.6 服务失效攻击 8.3 网络入侵攻击的典型过程 8.3.1 确定攻击目标并获取目标系统的信息 8.3.2 获取目标系统的一般权限 8.3.3 获取目标系统的管理权限 8.3.4 隐藏自己在目标系统中的行踪 8.3.5 对目标系统或其他系统发起攻击 8.3.6 在目标系统中留下下次入侵的后门 8.4 入侵检测系统的基本原理 8.4.1 入侵检测框架简介 8.4.2 网络入侵检测的信息来源 8.4.3 网络入侵检测信息分析 8.4.4 入侵检测的基本技术 8.5 入侵检测的基本方法 8.6 入侵检测系统的结构 8.6.1 基于主机的入侵检测系统 8.6.2 基于网络的入侵检测系统 8.6.3 分布武检测技术 8.7 实现入侵检测需

要考虑的问题 本章小结 习题 第9章 网络黑客技术及其利用方法 9.1 什么是黑客 9.1.1 黑客的定义和分类 9.1.2 黑客对网络信息系统的影响 9.1.3 黑客与法律 9.2 黑客常用的攻击方法和防范措施 9.2.1 黑客攻击的一般过程 9.2.2 信息探测 9.2.3 网络嗅探攻击技术 9.2.4 缓冲区溢出攻击 9.2.5 SQL注入式攻击 9.2.6 特洛伊木马攻击技术 9.3 黑客技术的可利用性 9.3.1 利用黑客技术对信患系统进行监管 9.3.2 促进对黑客技术的研究和利用 9.3.3 在信患战和情报战中使用黑客技术 本章小结 习题 第10章 VPN技术与IPSec协议 10.1 VPN技术及其应用 10.1.1 VPN概念 10.1.2 VPN的应用领域 10.2 VPN技术及其管理 10.2.1 VPN技术概览 10.2.2 VPN在TCP/IP协议层的实现 10.2.3 VPN的管理问题 10.3 安全VPN与网络安全 10.3.1 问题的提出 10.3.2 安全VPN的功能特性 10.4 链路层隧道封装技术 10.4.1 L2F协议 10.4.2 L2TP协议 10.4.3 PPTP协议 10.5 网际协议安全IPSec 10.5.1 IPSec概述 10.5.2 IPSec安全体系结构 10.5.3 IPSec安全机制 10.5.4 IPSec应用概述 本章小结 习题 附录一 缩略语对照表 附录二 Windows XP SP2默认安装的服务 参考文献

章节摘录

版权页：插图：1.加密机制 加密机制是各种安全服务和其他许多安全机制的基础，既能为数据提供机密性，也能为通信业务流信息提供机密性，并且还成为本节所述其他安全服务和安全机制中的一部分，能起到支持或补充作用。

(1) 加密层的选取 大多数应用将不要求在多个层上加密，加密层的选取主要取决于以下几个因素：

如果要求全通信业务流具有机密性，可选取物理层加密或传输安全手段（例如适当的扩频技术）。足够的物理安全、可信任的路由选择以及在中继上的类似机制能够满足所有的机密性要求。

如果要求细粒度的保护（例如对每个应用提供不同的密钥）、抗抵赖或选择字段的保护，可选取表示层加密。

由于加密算法会耗费大量的处理能力，因此选择字段的保护是很重要的。

在表示层中的加密能提供不带恢复的完整性、抗抵赖以及所有的机密性保护。

如果希望的是所有端系统到端系统通信的机密性保护，或者希望有一个外部的加密设备（例如为了给算法和密钥以物理保护或防止错误软件），可选取网络层加密。

它能够提供机密性与不带恢复的完整性。

虽然在网络层不提供恢复，但传输层正常的恢复机制能够用来恢复网络层检测到的攻击。

如果要求带恢复的完整性，同时又具有细粒度保护，可选取传输层加密，它能够提供机密性、带恢复的完整性或不带恢复的完整性。

对于今后的实施，不推荐在数据链路层上加密。

当关系到这些主要因素中的两项或多项时，可能需要在多个层上提供加密。

(2) 加密算法的类别 加密算法可以是可逆的，也可以是不可逆的。

可逆加密算法有两大类： 对称密码体制：知道了加密密钥也就意味着知道了解密密钥，反之亦然。

非对称密码体制：知道了加密密钥并不意味着也知道解密密钥，反之亦然。

这种系统的这两个密钥有时被称为“公钥”与“私钥”。

不可逆加密算法可以使用密钥，也可以不使用密钥。

若使用密钥，该密钥可以是公开的，也可以是秘密的。

(3) 密钥管理 除了某些不可逆加密算法的情况外，加密机制的存在意味着要使用密钥管理机制。

密钥管理涉及各个不同的阶段，其中包括密钥产生、密钥分配、密钥销毁、密钥取消等。

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>