

## <<信息系统安全概论>>

### 图书基本信息

书名：<<信息系统安全概论>>

13位ISBN编号：9787121082221

10位ISBN编号：7121082225

出版时间：2009-3

出版时间：石文昌、梁朝晖、沈昌祥 电子工业出版社 (2009-03出版)

作者：石文昌，梁朝晖 著

页数：463

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>

## <<信息系统安全概论>>

### 内容概要

本书以独特的方式讲授以主机为中心的系统安全的基本思想、技术和方法。

本书的宗旨是帮助读者认识每个人手中、家里、工作单位中、甚至庞大的数据处理中心深处的计算机主机系统的安全问题及其解决途径。

本书由三部分组成，第一部分是基础篇，包含第1~3章，内容包括信息系统安全绪论、计算机系统基础和可信计算平台基础等；第二部分是核心篇，包含第4~8章，内容包括操作系统的基础安全性、操作系统的增强安全性、数据库系统的基础安全性、数据库系统的增强安全性和系统完整性保护等；第三部分是拓展篇，包含第9~10章，内容包括基于主机的入侵检测和计算机病毒原理及其防治等。

本书的特色是透过信息网络空间的宏观安全体系结构去看待主机系统的安全问题，通过主机系统与信息安全知识体系的融合去认识主机系统的安全问题，采取核心硬件、系统软件和应用软件相结合的综合手段去分析主机系统的安全问题，运用安全性与可信性有机统一的整体措施去解决主机系统的安全问题，同时，本书注意体现网络环境对系统安全的影响及系统安全对整体安全的支撑。

本书可作为高等学校计算机、信息安全、电子与通信及相关专业的本科生和研究生的教材或参考书，也可供从事相关专业教学、科研和工程技术的人员参考。

## &lt;&lt;信息系统安全概论&gt;&gt;

## 书籍目录

第一部分 基础篇第1章 信息系统安全绪论1.1 安全攻击实景呈现1.1.1 诱惑及初探1.1.2 确定合适的突破口1.1.3 设法扩大战果1.1.4 全面出击1.1.5 尾声1.2 安全攻击环节概览1.2.1 侦察1.2.2 扫描1.2.3 获取访问1.2.4 维持访问1.2.5 掩盖踪迹1.3 信息安全典型事件1.4 信息安全经典要素1.4.1 机密性1.4.2 完整性1.4.3 可用性1.5 信息系统安全策略1.5.1 信息安全威胁1.5.2 策略与机制1.5.3 安全的目的1.5.4 安全策略的意义1.5.5 安全策略的类型1.6 信息系统访问控制1.6.1 访问控制矩阵1.6.2 访问控制的类型1.6.3 贝尔-拉普杜拉访问控制模型1.6.4 系统保护状态1.6.5 访问控制结构与设计原则1.7 系统安全知识定位1.7.1 系统安全的宏观定位1.7.2 系统安全的知识点定位1.8 本章小结习题1第2章 计算机系统基础2.1 程序员眼中的计算机系统2.1.1 计算机系统的硬件组成2.1.2 执行hello程序2.1.3 高速缓存2.1.4 层次结构的存储设备2.1.5 操作系统管理硬件2.1.6 通过网络与其他系统通信2.2 计算机组成基础2.2.1 中央处理单元2.2.2 主存储器2.2.3 输入/输出子系统2.2.4 子系统的内部连接2.3 操作系统基础2.3.1 操作系统的发展及其意义2.3.2 操作系统的演化2.3.3 操作系统的构成2.3.4 现代操作系统的特征2.3.5 Linux和Windows操作系统结构2.4 数据库系统基础2.4.1 数据模型2.4.2 概念模型2.4.3 关系模型2.4.4 数据库系统结构2.4.5 数据库系统的组成2.5 本章小结习题2第3章 可信计算平台基础3.1 可信计算发展概貌3.1.1 TCG可信计算的典型前期基础3.1.2 TCG可信计算的发展思路3.1.3 响应TCG规范的热点研究3.2 可信计算平台的基本特性3.2.1 保护能力3.2.2 对外证明3.2.3 完整性度量、存储和报告3.3 可信计算平台的基本体系3.3.1 平台的可信构件块3.3.2 信任边界3.3.3 信任传递3.3.4 完整性度量3.3.5 完整性报告3.3.6 以TPM为通信端点3.3.7 存储保护3.4 可信平台模块3.4.1 TPM的组件3.4.2 通信接口3.4.3 具有篡改保护能力的装配3.5 可信计算平台的隐私问题3.6 可信计算平台的运行模型3.6.1 TPM的工作状态3.6.2 平台的工作方法3.6.3 平台的软件接口3.6.4 TPM命令的授权验证3.7 可信计算平台的编程接口3.7.1 编程相关的TCG命名习惯3.7.2 程序员视角的TPM结构3.7.3 TPM的启动与清零3.7.4 在程序中使用TPM命令3.7.5 TPM命令的基本用途3.8 本章小结习题3第二部分 核心篇第4章 操作系统的基础安全性4.1 操作系统安全概貌4.1.1 操作系统安全简史4.1.2 操作系统安全的主要内容4.1.3 必不可少的操作系统安全性4.2 身份标识与认证的基本方法4.2.1 身份标识的基本方法4.2.2 身份认证的基本方法4.2.3 口令信息的管理方法4.3 面向网络的身份认证4.3.1 认证信息的网络化管理4.3.2 认证信息的加密传输4.3.3 面向服务的再度认证4.4 基于PAM的统一认证框架4.5 基于权限位的访问控制4.5.1 访问权限的定义与表示4.5.2 用户的划分与访问控制4.5.3 访问控制算法4.6 进程的有效身份与权限4.6.1 进程与文件和用户的关系4.6.2 进程的用户属性4.6.3 进程有效用户属性的确定4.7 基于ACL的访问控制4.7.1 ACL的表示方法4.7.2 基于ACL的访问判定4.8 特权分割与访问控制4.8.1 特权的意义与问题4.8.2 特权的定义4.8.3 基于特权的访问控制4.9 加密文件系统4.9.1 加密文件系统的应用方法4.9.2 加密文件系统的基本原理4.9.3 加密算法的加密密钥4.10 系统行为审计4.10.1 审计机制的结构4.10.2 审计指令的配置4.10.3 审计信息的分析4.11 本章小结习题4第5章 操作系统的增强安全性5.1 TE模型与DTE模型5.1.1 TE模型的基本思想5.1.2 DTE模型的基本思想5.2 SELinux实现的TE模型5.2.1 SETE模型与DTE模型的区别5.2.2 SETE模型的访问控制方法第6章 数据库系统的基础安全性第7章 数据库系统的增强安全性第8章 系统完整性保护第三部分 拓展篇第9章 基于主机的入侵检测第10章 计算机病毒原理及其防治参考文献

## <<信息系统安全概论>>

### 章节摘录

插图：第一部分 基础篇第1章 信息系统安全绪论兵法曰：知彼知己，百战不殆。

攻与防的对抗是信息安全的主题，了解安全攻击才能更好地进行安全防御。

本章以信息安全攻击的实景为起点，初步建立了信息安全攻击威胁的感性认识，开始体验信息安全的基本理念，并透过信息安全的攻击威胁感受系统安全在信息安全中的地位和作用。

本章主要由安全攻击实景呈现、安全攻击环节概览、信息安全典型事件、信息安全经典要素、信息系统安全策略、信息系统访问控制及系统安全知识定位等内容构成。

1.1 安全攻击实景呈现研究信息安全问题的目的是解决在现实应用中遇到的日益棘手的信息安全问题。本着“从实践中来，到实践中去”的思想，作为本章乃至本书的开始，下面讲述一个并非虚构的故事。

故事发生在一个发达国家，故事的主人公名叫卡尔，深谙信息安全攻击之法，他可不是一个喜欢通过恶作剧来炫耀自己的人，他实施信息安全攻击的意图非常明确，那就是获取经济利益。

1.1.1 诱惑及初探一个偶然的的机会，卡尔在媒体上看到了一篇有关某公司发展情况介绍的文章，那是一家销售精致小饰品的公司，据文章介绍，该公司发展非常迅速，一时间销售网点已遍布全国各地。

读了该介绍文章，卡尔顿时眼前一亮，似乎看到了商机。

他想：这家公司扩张得如此迅速，想必在网络信息系统建设中也许还来不及慎重考虑安全防范的问题，在信息安全方面应该是有机可乘的。

于是，卡尔盯上了该公司，从现在开始，我们不妨把该公司称为猎物公司，因为卡尔已经把它纳入了自己的攻击对象。

## <<信息系统安全概论>>

### 编辑推荐

《信息系统安全概论》的特色是透过信息网络空间的宏观安全体系结构去看待主机系统的安全问题，通过主机系统与信息安全知识体系的融合去认识主机系统的安全问题，采取核心硬件、系统软件和应用软件相结合的综合手段去分析主机系统的安全问题，运用安全性与可信性有机统一的整体措施去解决主机系统的安全问题，同时，《信息系统安全概论》注意体现网络环境对系统安全的影响及系统安全对整体安全的支撑。

<<信息系统安全概论>>

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>