

## <<信息系统安全教程>>

### 图书基本信息

书名：<<信息系统安全教程>>

13位ISBN编号：9787302151272

10位ISBN编号：730215127X

出版时间：2007-7

出版单位：清华大学

作者：张基温

页数：265

字数：400000

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>

## <<信息系统安全教程>>

### 内容概要

本书从应用的角度介绍信息系统安全原理，围绕防护、检测、响应和恢复，重点介绍了数据加密、认证技术、访问控制、入侵与攻击、网络防范和安全管理，内容覆盖了当前有关信息系统安全的基本技术。

书中不但提供了较为充分的习题，还设计了17个旨在提高学习者动手能力并发挥其创造性的实验。

本书深入浅出、富有哲理、结构新颖，紧扣理论本质，实践性强，适合学习，可以激发学生的学习热情。

本书适合作为计算机科学与技术专业、信息管理与信息系统专业和信息安全专业的“信息系统安全”课程的教材或教学参考书，也可供有关技术人员参考。

## &lt;&lt;信息系统安全教程&gt;&gt;

## 书籍目录

## 第0章 引论

## 0.1 信息系统风险

## 0.1.1 信息系统及其重要性

## 0.1.2 信息系统安全威胁

## 0.1.3 信息系统安全的脆弱性

## 0.1.4 风险 = 脆弱性+威胁

## 0.2 信息系统安全概念

## 0.2.1 基于通信保密的信息系统安全概念

## 0.2.2 基于信息系统防护的信息系统安全概念

## 0.2.3 基于信息保障的信息系统安全概念

## 0.2.4 基于经济学的信息系统安全概念

## 0.3 信息系统安全体系

## 0.3.1 OSI安全体系的安全服务

## 0.3.2 OSI安全体系安全机制

## 0.3.3 信息系统的安全管理

## 0.3.4 信息系统安全的防御原则

## 习题

## 第1章 数据保密

## 1.1 数据加密技术概述

## 1.1.1 替代密码

## 1.1.2 换位密码

## 1.1.3 简单异或

## 1.1.4 分组密码

## 1.1.5 对称密码体制和非对称密码体制

## 1.1.6 密钥的安全与公开密码体制

## 实验1 加密博弈

## 1.2 数据加密标准算法

## 1.2.1 DES及其基本思想

## 1.2.2 DES加密过程细化

## 1.2.3 关于DES安全性的讨论

## 1.2.4 其他对称加密算法

## 1.3 公开密钥算法RSA

## 1.3.1 RSA数学基础

## 1.3.2 RSA加密密钥的产生

## 1.3.3 RSA加密 / 解密过程

## 1.3.4 RSA安全性分析

## 实验2 RSA公开密钥系统的实现

## 1.4 密钥管理

## 1.4.1 密钥管理的一般过程

## 1.4.2 密钥分配方法举例

## 1.5 信息隐藏概述

## 1.5.1 信息隐藏的概念

## 1.5.2 信息隐藏处理过程

## 1.5.3 信息隐藏技术分类

## 习题

## <<信息系统安全教程>>

### 第2章 认证技术

#### 2.1 报文鉴别

##### 2.1.1 数据完整性保护概述

##### 2.1.2 报文鉴别与报文摘要数据完整性保护概述

##### 2.1.3 报文摘要算法

#### 实验3 实现报文认证算法

#### 2.2 数字签名

##### 2.2.1 直接数字签名和数字签名标准DSS

##### 2.2.2 有仲裁的数字签名

#### 实验4 加密软件PGP的使用

##### 2.2.3 应用实例——安全电子交换协议SET

#### 2.3 身份证明机制

##### 2.3.1 口令

##### 2.3.2 生物特征信息

##### 2.3.3 智能卡与电子钥匙身份验证

##### 2.3.4 数字证书

#### 2.4 认证协议

##### 2.4.1 单钥加密认证协议

##### 2.4.2 Kerberos认证系统

##### 2.4.3 公钥加密认证协议

##### 2.4.4 X.509标准

#### 实验5 证书制作及CA系统配置

#### 2.5 基于认证的Internet。

#### 安全

##### 2.5.1 IPsec

##### 2.5.2 SSL

##### 2.5.3 VPN

#### 实验6 实现一个VPN连接

#### 习题

### 第3章 访问控制

### 第4章 信息系统入侵与攻击

### 第5章 信息系统防卫

### 第6章 信息系统安全管理

### 参考文献

## &lt;&lt;信息系统安全教程&gt;&gt;

## 章节摘录

版权页：插图：信息系统是现代社会中一个重要的系统，信息系统也是一个复杂的系统。这些重要性和神秘感不断吸引着竞争对手的注意力，刺激着好奇者、好胜者和恶作剧者的兴趣。他们如八仙过海，千方百计地非授权地进入系统，各取所需，各显其功。

一般来说，可以采用信息系统入侵和攻击的手段有下面一些。

1. 恶意代码攻击 最常见的恶意代码是病毒。

病毒是潜入信息系统中的一些程序代码。

这些代码可以在未授权的情况下运行，或用来消耗系统资源，或用来搜集系统的敏感信息，或产生一些与系统工作无关的动作，或使系统丧失一些正常的功能。

除了病毒之外，还有其他类型的一些恶意代码，例如特洛伊木马、蠕虫、细菌、陷门、逻辑炸弹等。它们之间的区别在于需要不需要寄生在别的程序上（寄生性）、有没有自我复制能力（传染性），以及执行是否依赖某些条件（触发性）等特征上。

2. 消息收集攻击 收集被攻击系统的敏感信息或漏洞信息。

3. 代码漏洞攻击 任何程序系统都有一些薄弱环节。

这些薄弱环节可能来自设计上的疏忽，也可能来自配置或操作上的错误，也可能来自系统管理上的不足。

系统的漏洞一旦被人侵者发现或掌握，就有可能被利用向系统发起攻击。

4. 欺骗和会话劫持攻击 欺骗与会话劫持也属于系统漏洞攻击的一种。

但是，一般说漏洞指操作系统和其他系统软件中的薄弱环节，而欺骗和会话劫持由于利用计算机网络中的开放性和身份认证的不完全性，使得攻击者可以假冒别人身份进行活动的攻击行为。

5. 分布式攻击 计算机网络本身是一种分布式计算资源。

分布式攻击就是攻击者利用这种资源进行的系统攻击行为。

例如利用这种分布式计算资源进行口令猜测、信息收集以及发起对某站点的“人海战术”攻击。

6. 其他攻击 常言道，道高一尺，魔高一丈。

信息系统安全是针对入侵和攻击采取的一系列安全策略和技术。

然而，按照木桶原理，当一块短的木板被加长后，另一块次短的木板就变成最短的木板了。

而一种攻击被防御之后，新的攻击又会出现。

防与攻的博弈将在竞争中永无止境。

4.1 计算机病毒 4.1.1 计算机病毒的特征 在生物学界，病毒（virus）是一类没有细胞结构但有遗传、复制等生命特征，主要由核酸和蛋白质组成的有机体。

计算机病毒（computer virus）有一些与生物界中的病毒极为相似的特征，这也就是称其为病毒的缘由。

下面介绍计算机病毒的一些基本特征。

1. 非授权执行性 通常，一个正常的程序被调用时，就要从系统获得控制权，得到系统分配的相应资源，使其执行对用户是透明的。

计算机病毒虽然具有正常程序所具有的一切特性，但是其执行是非授权进行的：它隐蔽在合法程序和数据中，当用户运行正常程序时，病毒伺机取得系统的控制权，先于正常程序执行，并对用户呈透明状态。

2. 感染性 与生物界中的病毒可以从一个生物体传播到另一个生物体一样，传染是病毒最本质的特征之一，是病毒的再生机制。

在单机环境下，计算机病毒的传染基本途径是通过磁盘引导扇区、操作系统文件和应用文件进行传染。

在网络中，计算机病毒主要是通过电子邮件、Web页面等特殊文件和数据共享方式进行传染。

3. 潜伏性与隐蔽性 病毒程序一旦取得系统控制权，可以在极短的时间内传染大量程序。

但是，被感染的程序并不是立即表现出异常，而是潜伏下来，等待时机。

计算机病毒的潜伏还依赖于其隐蔽性。

为了隐蔽，病毒通常非常短小（一般只有几百或1K字节，此外还寄生于正常的程序或磁盘较隐蔽的地方，也有个别病毒以隐含文件形式存在，使人们不经过代码分析很难被发觉。

<<信息系统安全教程>>

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>