Information Security

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI

普通高等学校信息安全“十一五”规划教材

计算机信息系统安全实验教程

JISUANJI XINXI XITONG ANQUAN SHIYAN JIAOCHENG

鲁 珂 赵继东 董宇亮 编著

杨国纬 主审

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI
普通高等学校信息安全"十一五"规划教材

计算机信息系统安全实验教程

鲁 珂 赵继东 董宇亮 编著

杨国纬 主审

电子科技大学出版社

图书在版编目（CIP）数据

计算机信息系统安全实验教程 / 鲁珂等编著. —成都：电子科技大学出版社，2007.3

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-228-0

Ⅰ. 计… Ⅱ. 鲁… Ⅲ. 电子计算机—信息系统—安全技术—高等学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 024719 号

内 容 提 要

本书为普通高等学校信息安全“十一五”规划教材之一，内容丰富，实验设计新颖实用，涵盖了当前计算机信息系统安全方面主流的攻防技术，共设计了 20 多个具体的实验。涉及的主要安全技术有：计算机病毒及反病毒技术、系统缓冲区漏洞分析及利用技术、软件破解及反破解技术、系统控制及隐藏技术、公开密钥加密机制及文件加密技术等。

本书既可作为信息安全或计算机专业本科生、专科生的实验教材，也可作为相关领域专业技术人员的参考用书。

普通高等学校信息安全“十一五”规划教材

计算机信息系统安全实验教程

鲁 珂 赵继东 董宇亮 编著

杨国纬 主审

出 版： 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）

策划编辑： 曾 艺

责任编辑： 曾 艺

主 页： www.uestcp.com.cn

电子邮箱： uestcp@uestcp.com.cn

发 行： 新华书店经销

印 刷： 成都蜀通印务有限责任公司

成品尺寸： 185mm×260mm 印张 19.25 字数 468 千字

版 次： 2007 年 3 月第一版

印 次： 2007 年 3 月第一次印刷

书 号： ISBN 978-7-81114-228-0

定 价： 30.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

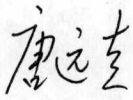
秦志光　李建平　周明天

序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。



二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

前言

计算机信息系统安全问题的研究范围包括信息安全、网络安全和系统安全等多个方面，是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。网络时代的计算机信息系统安全形势十分复杂，面临着许多重大的安全威胁。为了成功解决不断出现的各种安全问题，需要相关人员具有深厚的专业基础知识，同时还需要具备较强的动手实践能力。

本书立足于当前计算机信息系统安全中的一些基本问题，如病毒入侵、黑客攻击等，共编写了 21 个实验。从总体上看，这些实验基本上覆盖了当前信息系统安全的主要领域。由于 Windows 操作系统在 PC 机上的垄断地位，再加上 Microsoft 提供的办公软件、数据库软件的通用性，使得现有的信息系统大多数都建立在 Windows 操作系统基础上，因此本书的所有实验均基于 Windows 平台设计，这样既能使我们的实验与实际更接近，同时也便于实验平台的统一。本书中的每个实验都是按照这种模式编写的：先给出有关的基础原理介绍，然后具体讲述实验的准备过程，再演示出具体的实验过程，最后进行实验的分析及讨论。为便于教学，在介绍一些相关的基础知识后，本书按病毒及反病毒技术、Windows 系统攻击与防御技术、Windows 系统防范技术、Windows 系统控制技术将实验组织为 4 个小节，每章实验按由浅入深的顺序介绍，教师可以选择其中一部分让学生完成，也可以让不同水平的学生做不同层次的实验。另外，本书的一些实验内容比较敏感，为防止用于其他目的，本书没有附带源代码光盘，如果教师需要源代码用于教学目的，可以与本书作者(luke_74@163.com)联系获取。

在本书的写作过程中，在概述部分我们参考了四川大学信息安全研究所方勇教授的《信息系统安全导论》中的部分内容，在此表示感谢。本书由鲁珂老师、赵继东老师和董宇亮老师共同编写，并由鲁珂老师统稿。另外，田永宏、卢陈、肖勇、周艳、张乐乐、翟刚贺、姚博、张旭等研究生也参加了一些范例的验证和文字工作。对他们的辛勤劳动谨表感谢。我们引用了一些比较成功的案例，努力在参考文献中予以列出，在此向他们表示感谢。但是，有些资料（特别是网络资料）的来源并不是很清晰，或许也会有所错漏，谨在此致以歉意。

计算机信息系统安全是一门非常年轻的课程，它的内容尚在不断发展之中，它的架构也还在摸索之中，其实验课程更是刚刚开始。由于能力和水平所限，教材中必然会有许多缺点和不足，甚至还有不少错误，我们衷心期望有关专家和同仁，特别是使用过本书的教师、学生能毫无保留地提出所发现的问题和改进建议。我们将会在修订时将他们对本书的贡献铭记在前言中。

鲁　珂

2007.1

目录

第 3 章　PE 病毒及反病毒技术相关实验

目录

第 4 章　Windows 系统攻击技术相关实验

第 5 章 Windows 系统防范技术相关实验

第1章

计算机信息系统安全概述

1.1 计算机信息系统的定义

信息系统是指用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和。

上述定义可以看成是广义的信息系统的定义。随着时代的发展，计算机的出现大大提高了信息处理的能力，计算机在信息存储和处理方面已经成为了一个基本的载体和工具。在现有条件下，绝大部分信息系统均建立在计算机系统基础上，依靠计算机上的各种软件来进行工作。

根据《中华人民共和国计算机信息系统安全保护条例》中的定义，信息系统（Information System）是指由计算机及其相关和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。这一定义表明在当前技术条件下，信息系统的构成将以计算机系统和网络系统为主，因此，除非特别指明，通常所称的信息系统实际上是计算机信息系统的简称。

1.2 计算机信息系统安全简介

1.2.1 计算机信息系统安全的定义

方勇等编著的《信息系统安全导论》中将信息系统安全定义为：确保以电磁信号为主要形式的、在计算机网络化（开放互联）系统中进行自动通信、处理和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。这里的人指信息系统的主体，包括各类用户、支持人员，以及技术管理和行政管理人员；网络则指以计算机、网络互联设备、传输介质、信息内容及其操作系统、通信协议和应用程序所构成的物理的与逻辑的完整体系；环境则是系统稳定和可靠运行所需要的保障体系，包括建筑物、机房、动力保障与备份，以及应急与恢复体系。

伴随着计算机技术和网络通信技术的飞速发展，计算机信息系统日益庞大，构成系统的实体数量、实体类型、网络结构、信息流方式、信息处理方式等都发生了非常大的变化，成为一个庞大的复杂系统。该系统涉及国家的政治、军事、文教等诸多领域，其中存储、传输和处理的信息中有很多，如政府宏观调控决策信息、银行资金转账信息、股票证券信息、商业经济信息、能源资源数据和科研数据等是重要信息、敏感信息，甚至是国家机密，因此难免会吸引来自世界各地的各种人为攻击（例如窃取信息、篡改数据、假冒信息、伪造信息等）。另一方面，随着计算机犯罪的迅速增加，各国的计算机信息系统都面临着很大的威胁，并成为严重的社会问题之一，因此各国在信息系统安全方面都在不断加大研究力度。同时，随着计算机信息系统规模的不断扩大，结构的日趋复杂，信息的共享程度越来越高，计算机信息系统安全问题的研究范围也越来越广，它已涉及信息安全、网络安全和

系统安全多个方面，是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。从广义上讲，凡是涉及计算机及其相关的配套设备、设施（含网络）上的信息的保密性、完整性、可用性、认证性和不可否认性的相关技术和理论都是计算机信息系统安全的研究领域。

1.2.2 信息系统自身的安全脆弱性

信息系统本身由于系统主体和客体的原因可能存在不同程度的脆弱性，就为各种动机的攻击提供了入侵、骚扰或破坏信息系统的途径和方法。所谓信息系统的脆弱性，是指信息系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因而可能导致系统受到破坏、更改、泄露和功能失效，从而使信息系统处于异常状态，甚至崩溃瘫痪等。具体分析如下：

1. 硬件组件

信息系统硬件组件的安全隐患多来源于设计，主要表现为物理安全方面的问题。各种计算机或网络设备（如主机、CRT、电缆、hub、路由器、微波线路等），除难以抗拒的自然灾害外，温度、湿度、尘埃、静电、电磁场等也可以造成信息的泄露或失效。信息系统在工作时，向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2. 软件组件

软件组件的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及软件过长、过大，不可避免地存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件，这种软件从安全角度看是绝对不可用的。

软件组件可分为三类，即操作平台软件、应用平台软件和应用业务软件。这三类软件以层次结构构成软件组件体系。操作平台软件处于基础层，维系着系统组件运行的平台，因此操作平台软件的任何风险都可能直接危及或被转移或延伸到应用平台软件。所以，对信息系统安全所需的操作平台软件的安全等级要求不得低于系统安全等级要求，特别是信息系统的安全服务组件的操作系统安全等级必须至少高于系统安全一个等级，强烈建议安全服务组件的操作系统不得直接采用商业级或普遍使用的操作系统。应用平台软件处于中间层次，是在操作平台支撑下运行的支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可直接危及或传递给应用业务软件。因此应用平台软件的安全特性也至关重要。在提供自身安全保护的同时，应用平台软件还必须为应用软件提供必要的安全服务功能。应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险都直接表现为信息系统的风险，因此其安全功能的完整性及自身的安全等级，必须大于系统安全的最小需求。一般来说，外购的商业化应用软件比自制应用业务软件更安全些。

3. 网络和通信协议

在当今的网络通信协议中，局域网和专用网络的通信协议具有相对封闭性，因为它不能直接与异构网络连接和通信。这样的“封闭”网络本身基于两个原因比开放式的 Internet 的安全特性好，一是网络体系的相对封闭性降低了从外部网络或站点直接攻入系统的可能性，但信息的电磁泄露性和基于协议分析的搭线截获问题仍然存在；二是专用网络自身具有较为完善、成熟的身份鉴别，访问控制和权限分割等安全机制。

安全问题最多的网络和通信协议是基于 TCP/IP 协议栈的 Internet 及其通信协议。因为任何接入 Internet 的计算机网络协议以及利用公共通信基础设施构建的内联网/外联网，在理论上和技术实践上已无真正的物理界限，同时在地缘上也没有真正的国界。国与国之间、组织与组织之间，以及个人与个人之间的网络界限是依靠协议、约定和管理关系进行逻辑划分的，因而是一种虚拟的网络现实；而且支持 Internet 运行的 TCP/IP 协议栈原本只考虑互联互通和资源共享的问题，并未考虑也无法兼容解决来自网际中的大量安全问题。Internet 何以存在如此多的安全隐患，TCP/IP 协议栈到底有哪些脆弱性和漏洞？要理解与 Internet 有关的安全脆弱性和漏洞存在的原因和分布情况，需从网络技术发展历史和 TCP/IP 协议栈的研究初衷、使用背景及发展驱动力等方面分析。

（1）缺乏对用户身份的鉴别

TCP/IP 协议的机制性安全隐患之一是缺乏对通信双方真实身份的鉴别机制。由于 TCP/IP 协议使用 IP 地址作为网络节点的唯一标识，而 IP 地址的使用和管理又存在很多问题，因而可导致下列两种主要安全隐患：

- IP 地址是由 Internet 信息中心（InterNIC）分发的，其数据包的源地址很容易被发现，且 IP 地址隐含了所使用的子网掩码，攻击者据此可以画出目标网络的轮廓。因此使用标准 IP 地址的网络拓扑对 Internet 来说是暴露的。
- IP 地址很容易被伪造和被更改，且 TCP/IP 协议没有对 IP 包中源地址真实性的鉴别机制和保密机制。因此 Internet 上任何主机都可以产生一个带有任意源 IP 地址的 IP 包，从而假冒另一个主机进行地址欺骗。

（2）缺乏对路由协议的鉴别认证

TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护。因此可以通过 Internet 利用路由信息修改网络传输路径，误导网络分组传输。

（3）TCP/UDP 的缺陷

TCP/IP 协议规定了 TCO/UDP 是基于 IP 协议上的传输协议，TCP 分段和 UDP 数据包是封装在 IP 包中在网上传输的，除可能面临 IP 层所遇到的安全威胁外，还存在下列 TCP/UDP 实现中的安全隐患：

- 建立一个完整的 TCP 连接，需要经历“三次握手”过程。在客户/服务器模式的“三次握手”过程中，假如客户的 IP 地址是假的，是不可达的，那么 TCP 不能完成该次连接所需的“三次握手”，使 TCP 连接处于“半开”状态。攻击者利用这一弱点可实施如 TCP SYN Flooding 攻击的“拒绝服务”攻击。
- TCP 提供可靠连接是通过初始序列号和鉴别机制来实现的。每一个合法的 TCP 连接都有一个客户/服务器双方共享的唯一序列号作为标识和鉴别。初始序列号一般由随机数发生器产生，但问题出在很多操作系统（如 UNIX）在实现 TCP 连接初始序列号的方法中，

所产生的序列号并不是真正随机的，而是一个具有一定规律、可猜测或计算的数字。对攻击者来说，猜出了初始序列号并掌握了目标 IP 地址之后，就可以对目标实施 IP Spoofing 攻击，而 IP Spoofing 攻击很难检测，因此此类攻击危害极大。

- UDP 是一个无连接控制协议，极易受 IP 源路由和拒绝服务型攻击。
- 在 TCP/IP 协议层结构中，应用层位于最顶部，因此下层的安全缺陷必然导致应用层的安全出现漏洞甚至崩溃；而各种应用层服务协议（如 Finger，FTP，Telnet，E-mail，DNS，SNMP 等）本身也存在许多安全隐患，这些隐患涉及鉴别、访问控制、完整性和机密性等多个方面，极易引起针对基于 TCP/IP 应用服务协议和程序方面安全缺陷的攻击并获得成功。

1.2.3 对信息系统安全的威胁

需要指出的是，威胁信息系统安全的因素是多方面的，目前还没有统一的方法对各种威胁加以区别和进行准确的分类。而且不同威胁的存在及其重要性是随环境的变化而变化的。下面是对现代信息系统及网络通信系统常遇到的一些威胁及其来源的概述。

1. 基本威胁

信息安全的基本目标是实现信息的机密性、完整性、可用性和资源的合法使用。对信息系统这四个基本安全目标的威胁即是基本威胁。

（1）信息泄露

信息泄露指敏感数据在有意或无意中被泄露、丢失或透露给某个未授权的实体。它通常包括：信息在传输中被丢失或泄露（如利用电磁泄露或搭线窃听等方式可截获机密信息）；通过对信息流向、流量、通信频度和长度等参数的分析，推测出有用信息（如用户口令、账号等重要信息）。

（2）完整性破坏

以非法手段窃得对信息的管理权，通过未授权的创建、修改、删除和重放等操作而使数据的完整性受到破坏。

（3）服务拒绝

信息或信息系统资源的利用价值或服务能力下降或丧失。这可能由两方面的原因造成：一是受到攻击所致。攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的系统负载，从而导致系统的资源对合法用户的服务能力下降或丧失。二是由于信息系统或其组件在物理上或逻辑上受到破坏而中断服务。

（4）未授权访问

未授权实体非法访问信息系统资源，或授权实体超越权限访问信息系统资源。例如，有意避开系统访问控制机制，对信息设备及资源进行非法操作或运行；擅自扩大权限，越权访问信息系统资源。非法访问主要有假冒和盗用合法用户身份攻击、非法进入网络系统进行违法操作，合法用户以未授权的方式进行操作等形式。

2. 威胁信息系统的主要方法

在对信息系统的安全威胁中，某些方法常常被大量使用，因为这些方法具有易学性和