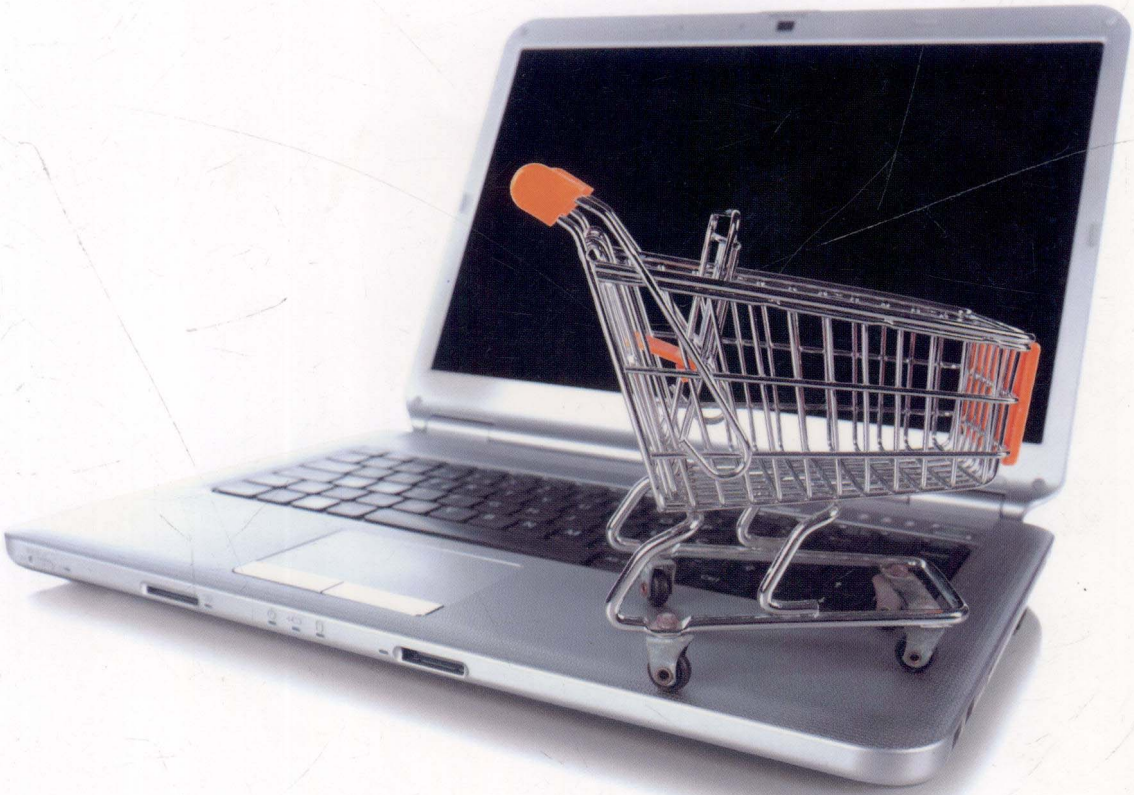
21 世纪本科财经管理类专业实验与实践系列规划教材
丛书主编◎胡巧多



电子支付与信息安全实践教程

主　编◎张新谊
副主编◎叶　龙

清華大學出版社

21世纪本科财经管理类专业实验与实践系列规划教材
丛书主编：胡巧多

电子支付与信息安全实践教程

张新谊　主　编
叶　龙　副主编

清华大学出版社
北京

内 容 简 介

本书是为高校非计算机专业学生特别撰写的。它结合现场的实验软硬件环境，并充分考虑了学生的培养特点以及将来就业的社会需求，力求让学生通过实验实践，完善电子支付与信息安全的理论学习，更加深入理解电子支付与信息安全的意义和作用。

本书共分 8 章，分别为操作系统篇、网络系统安全篇、病毒篇、应用安全篇、数据库篇、电子商务应用篇、电子商务环境搭建与营销支付篇和电子商务物流篇，本书还提供了 13 个实验供学生练习。

真实、体验、直观是本书的特色，通过本书的学习和交流，可使学生在实际环境中动手操作，并从实践中检验知识。

本书既可作为高校非计算机各专业的实验教材，也可作为高职高专各专业的实验教材，还可作为其他专业人员的参考书。

图书在版编目(CIP)数据

电子支付与信息安全实践教程/张新谊主编. --北京：清华大学出版社，2012.7
(21 世纪本科财经管理类专业实验与实践系列规划教材)
ISBN 978-7-302-28651-6

Ⅰ. ①电… Ⅱ. ①张… Ⅲ. ①电子商务－支付方式－高等学校－教材 ②电子商务－安全技术－高等学校－教材 Ⅳ. ①F713.36

中国版本图书馆 CIP 数据核字(2012)第 077065 号

责任编辑：索　梅　王冰飞
封面设计：史　墨
责任校对：时翠兰
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：10.25　　**字　数**：221 千字
版　　次：2012 年 7 月第 1 版　　**印　次**：2012 年 7 月第1 次印刷
印　　数：1～3000
定　　价：19.50 元

产品编号：041855-01

21世纪本科财经管理类专业实验与实践系列规划教材

编写委员会成员

主　任：冯伟国

副主任：陶　田　胡巧多

委　员（按姓氏笔画）：

马燕林　王云玺　王胜桥　刘建民
刘　斌　池丽华　吴晓伟　张士英
张　影　李相波　陈尹立　周　勇
侯立玉　姜　红　黄都培

序

PREFACE

目前，我国财经类院校在人才培养过程中比较注重专业知识和技能的传授与培养，而对跨专业的行业通识教育重视不足。本套教材是上海商学院在几年探索与实践基础上，逐步形成的经管类各专业通识性教育系列实践教材。

本套教材由长期从事财经类专业教学一线教师与企业专家共同编写。教材主要包括信息管理类、营运资金管理类、人力资源管理类、商贸应用扩展类和技能培训类五大模块的实验实训内容。通过本套教材学习，学生可以具备经管类跨专业的基本素养，为以后的职业发展打下扎实的实践基础。为了更好地训练学生自主学习能力，本套教材还配套编写了支持学生自主学习的网络实践学习指导。本套教材可用于财经类本科学校普适性实践教学。

胡巧多

2012 年 5 月

前言

FOREWORD

信息技术的高速发展给社会发展带来重大影响，也严重影响了人们的生产和生活。人们对信息的依赖越来越大，同样，人们对信息的安全也提出了更高的要求。

信息化给人们带来新的社会安全问题，尤其以网络环境为中心的信息系统的安全问题不同于传统意义的安全，它具有新的形势和特点。无论是在信息安全管理方面，还是在电子商务应用技术方面，人才是核心要素，需要不同领域、不同层次的多方面人才，特别是高素质复合型人才尤为重要。

本书为高校非计算机专业学生特别撰写，它结合了现场实验的软硬件环境，并充分考虑了学生的培养特点以及将来就业的客观社会需求，力求让学生通过实验实践，将理论知识与实际应用相结合。

真实、体验、直观是本书的特色。

本书共分 8 章，分别为操作系统篇、网络系统安全篇、病毒篇、应用安全篇、数据库篇、电子商务应用篇、电子商务环境搭建与营销支付篇和电子商务物流篇，每章前均有相关的理论知识的介绍。本课程建议学时为 32～36 学时，同时共附有 13 个实验，在实际教学过程中，可根据学生的具体情况和学时，做适当的删减，建议每章至少完成一个实验。

本书由张新谊任主编，蒋传进编写了第 6 章、第 7 章和第 8 章，蔡京玫编写了第 3 章，叶龙编写了第 5 章，其余由张新谊编写并统稿。

在本书的编写过程中，得到了上海庚商网络信息技术有限公司和南京奥派信息技术有限公司的大力支持，在此一并致谢。

由于编者水平所限，书中一定存有不足之处，敬请读者提出宝贵意见和建议。

编　者

2012 年 3 月于上海

目录

CONTENTS

第1章

操作系统篇

1.1 引言

操作系统是计算机中最基础、最重要的系统软件，各种应用程序要想运行，必须依赖于操作系统提供的系统软件，没有安全操作系统的支撑，安全保密性也就无从谈起。利用 Windows Server 2003 系统自身的安全工具，通过身份验证、账户管理、权限管理、日志管理等可以制定一套完善的计算机安全防护策略，维护 Windows 操作系统的基本安全。

1.2 操作系统概述

1.2.1 操作系统的功能

操作系统的主要功能，可以从以下三个方面来讨论：

(1) 管理计算机系统的硬件、软件、数据等各种资源，尽可能减少人工分配资源的工作以及人对机器的干预，发挥计算机的自动工作效率。

(2) 协调各种资源在使用过程中的关系，使得计算机的各种资源使用调度合理，高速设备与低速设备运行相互配合。

(3) 为用户提供使用计算机系统的环境，方便使用计算机系统的各部件或功能。操作系统通过自己的程序，将计算机系统的各种资源所提供的功能抽象出来，形成与之等价的操作系统的功能，并形象地表现出来，提供给用户，让其方便地使用计算机。

1.2.2 操作系统的分类

从用途的角度，操作系统可分为专用操作系统和通用操作系统两类。专用操作系统

是指用于控制和管理专项事物的操作系统，如现代手机中使用的操作系统，这类系统一般以嵌入硬件的方式出现，用于特定的用途。通用操作系统具有完善的功能，能够适应多种用途的需要。

从单机和网络的角度，操作系统可分为单机操作系统和网络操作系统。单机操作系统是针对单个计算机系统的环境设计的，它只有管理本机系统资源的功能。单用户操作系统是一种更为特殊的单机操作系统，它是针对一台机器、一个用户而设计的操作系统，它的基本特征是一次只能支持一个用户作业的运行，系统的所有资源由该用户独占，该用户对整个计算机系统有绝对的控制权。

从功能的角度，操作系统可分为批处理操作系统、分时操作系统、实时操作系统、网络操作系统、分布式操作系统。批处理操作系统、分时操作系统和实时操作系统的运行环境大多是单计算机系统，而网络操作系统和分布式操作系统的运行环境是多计算机系统。

1. 批处理操作系统

批处理操作系统的基本特征是“批量”，即将要交给计算机处理的若干个作业组织成队列成批地交给计算机自动地按作业队列顺序逐个处理。它可分为单道批处理操作系统和多道批处理操作系统。单道批处理操作系统一次只能调入一个处理作业在计算机内运行，其他作业放在辅助存储器上，它类似于单用户操作系统。计算机在运行处理作业时，时间主要消耗在两个方面：一方面是消耗在 CPU 执行程序上；另一方面是消耗在输入输出上。由于输入输出设备的速度相对于 CPU 执行程序的速度慢很多，导致计算机在输入输出时 CPU 处于空闲状态。为了提高 CPU 的使用效率，出现了多道批处理操作系统。它与单道批处理操作系统的区别是在计算机内存中可以有多个作业存在，调度程序根据事先确定的策略，选择一个作业将 CPU 资源分配给它运行处理，当处理的作业要进入输入输出操作时，就释放对 CPU 的占有，调度程序则从内存中等待处理的作业中选择一个交给 CPU 执行，这样，就提高了 CPU 的使用效率。

2. 分时操作系统

分时是指两个或两个以上的事件按时间划分轮流使用计算机系统的某一资源（主要是 CPU 资源）。在一个系统中如果多个用户分时使用一个计算机，那么这样的系统称为分时操作系统。分时的时间单位称为时间片，一个时间片一般是几十毫秒。在一个分时操作系统中，往往要连接几十个甚至上百个终端，每个用户在自己的终端上控制其作业的运行。通过操作系统的管理，将 CPU 轮流分配给各个用户使用。

3. 实时操作系统

实时操作系统要求实时处理并快速给出处理结果。实时操作系统一般是采用时间驱动的设计方法，系统能够及时对随时发生的事件做出响应并及时处理。实时操作系统分为实时控制操作系统和实时处理操作系统。实时控制操作系统常用于工业控制，以及飞行器、导弹发射等军事方面的自动控制。实时处理操作系统常用于预订飞机票、航班

查询，以及银行之间账务往来等。

4. 网络操作系统

随着计算机技术的迅速发展和网络技术的日益完善，不同地域的、具有独立处理能力的多个计算机系统通过通信设施互联，实现资源共享，组成计算机网络，成为一种更开放的工作环境，网络操作系统也应运而生。网络操作系统除了具有单机操作系统的所有功能以外，还具有网络资源的管理功能，支持网络应用程序运行。

5. 分布式操作系统

分布式操作系统是为分布式计算机系统配置的操作系统。分布式计算机系统与计算机网络一样，多台计算机系统通过通信网络互联，实现资源共享，但不同的是系统中的各个计算机没有主次之分，各计算机具有相对的自治性，用户访问共享资源时，不需要知道该共享资源位于哪台计算机上，如需要的话，系统中的多台计算机可以相互协作共同完成一个任务，即可以将一个任务分割成若干个子任务分散到多台计算机上同时并行执行。实际上，一种商用操作系统往往包括了批处理操作系统、分时操作系统、实时操作系统、网络操作系统、分布式操作系统等多方面的功能。不同的操作系统根据自身用途的定位和面向的用户，在各种功能的强弱上会有所区别。

1.3　Windows Server 2003 安全策略

随着信息化进程的加快，网络迅速发展，网络安全的重要性也渐渐凸现。网络安全涉及各个方面，而网络操作系统的安全设置很关键，Windows Server 2003 网络操作系统用户众多，是各种网络建设的首选，Windows Server 2003 网络操作系统沿袭了 Windows 的传统，在网络管理方面引入许多新的功能，提供了更高的硬件支持和更加强大的安全功能，如何用好 Windows Server 2003 的安全策略，怎样选择合理的设置，使网络安全配置得更好，对企业网、校园网、政务网等是至关重要的，要设置好 Windows Server 2003 网络操作系统的安全配置，必须了解 Windows Server 2003 网络操作系统的安全策略，分析 Windows Server 2003 网络操作系统的安全策略。

1.3.1　账户安全策略

账户安全策略包括密码策略、账户锁定策略和 Kerberos 策略三个方面，用户账户的保护主要是密码保护。通常采取提高密码的破解难度、启用账户锁定策略、限制用户登录等措施。密码策略用于域账户或本地用户账户。在 Windows Server 2003 系统中，可以通过账户策略设置中的“密码策略”来进行设置。通过提高密码的复杂性、增大密码的长度、提高更换频率等措施来提高密码的破解难度。该策略通过确保旧密码不能在某段时间内重复使用，使用户账户更安全。

要维持密码历史记录的有效性，则在通过启用密码最短使用期限安全策略，设置更改密码之后，不允许立即更改密码。可将密码的过期天数设置为 1～999 天；如果将天数

设置为0，则指定密码永不过期。使密码每隔30～90天过期一次是一种较好的安全选择。用这种方式，攻击者只能够在有限的时间内破解用户密码并访问网络资源。账户锁定策略用于域账户或本地用户账户，包含账户锁定时间、账户锁定阈值，以及复位账户锁定计数器。账户锁定是指在某些情况下为保护该账户的安全而将此账户进行锁定。使其在一定的时间内不能再次使用，从而挫败连续的猜解尝试。账户锁定时间确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围为0～99 999分钟。如果将账户锁定时间设置为0，那么在管理员明确将其解锁前，该账户将被锁定。如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间，默认值为无。因为只有当指定了账户锁定阈值时，该策略设置才有意义。账户锁定阈值，该安全设置确定造成用户账户被锁定的登录失败尝试的次数。无法使用锁定的账户，除非管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为0～999。如果将此值设为0，则将无法锁定账户。复位账户锁定计数器，该安全设置确定在登录尝试失败计数器被复位为0（即0次失败登录尝试）之前，尝试登录失败之后所需的分钟数。有效范围为1～99 999分钟。如果定义了账户锁定阈值，则该复位时间必须小于或等于账户锁定时间。Windows Server 2003系统在默认情况下，这种锁定策略并没有进行设定，对黑客的攻击没有任何限制。账户锁定策略设定的第一步就是指定账户锁定的阈值，即锁定前该账户无效登录的次数。一般设置账户锁定阈值为3次，如果3次登录全部失败，就会锁定该账户。Kerberos V5身份验证协议是用于确认用户或主机身份的身份验证机制，也是Windows Server 2003系统默认的身份验证服务。为防止“轮番攻击”，Kerberos V5在其协议定义中使用了时间戳。为使时间戳正常工作，客户端和域控制器的时钟应尽可能地保持同步。如果客户端时钟和域控制器时钟间的差值小于该策略中指定的最大时间差，那么在这两台计算机的会话中使用的任何时间戳都将被认为是可信的。

1.3.2 本地策略

本地策略包含审核策略、公钥策略、软件限制策略等。审核策略包含9个策略选项。系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障，以及各类安全事件。对Windows Server 2003系统来说，为了不影响系统性能，默认的安全策略并不对安全事件进行审核。从“安全配置和分析”工具用SecEdit安全模板进行的分析结果可知，这些有红色标记的审核策略应该已经启用，这可用来发现来自外部和内部的黑客的入侵行为。对于关键的应用服务器和文件服务器来说，应同时启用剩下的安全策略。如果已经启用了“审核对象访问”策略，那么就要求必须使用NTFS文件系统。NTFS文件系统不仅提供对用户的访问控制，而且还可以对用户的访问操作进行审核。但这种审核功能，需要针对具体的对象来进行相应的配置。首先在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组。在该对话框中选择好要审核的用户后，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，就可以通过检查系统的日志来发现黑客的蛛丝马迹。

在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机了。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。在 Windows Server 2003 IIS 6.0 中，其日志功能默认已经启动，并且日志文件存放的路径默认在 System32/LogFiles 目录下，打开 IIS 日志文件，可以看到对 Web 服务器的 HTTP 请求，IIS 6.0 系统自带的日志功能从某种程度上可以成为入侵检测的得力帮手。使用 Syskey 保障密码信息的安全。保存在活动目录中的域账号密码信息是最为敏感的安全信息。系统密钥(System Key，Syskey)就是用来加密保存在域控制器的目录服务数据库中的账号密码信息的。Syskey 一共有三种工作模式。一是所有 Windows Server 2003 中默认采用的，计算机随机产生一个系统密钥，并将密钥加密后保存在本地。在这种模式中，可以像平时一样地登录本地计算机。二是系统密钥使用和模式一中的生成方式和存储方式相同，但是它使用一个由管理员指定的附加密码以提供更进一步的安全性。当重新启动计算机时，必须在启动的时候输入管理员指定的附加密码，这个密码不保存在本地。三是安全性最高的操作方法，计算机随机产生的系统密钥将被保存在一张软盘上，而不是本地计算机。如果没有软盘的物理访问权限，并在系统提示时插入该软盘，就无法引导系统。保护域控制器是网络安全策略中的重要一步。

1.3.3　IPSec 策略

IPSec 策略是安全联网的长期方向。它通过端到端的安全性来提供主动的保护，为防止专用网与 Internet 的攻击提供了主要防线，在源 IP 地址和目标 IP 地址之间建立信任和安全性。IPSec 策略由常规 IPSec 策略设置和 IPSec 策略规则组成。由于在 IP 协议设计之初并没过多考虑安全问题，因此早期的网络中经常发生遭受攻击或机密数据被窃取等问题。为了增强网络的安全性，IP 安全(IPSec)协议应运而生。

为了增强网络通信安全或对客户机器的管理，网络管理员可以通过在 Windows 系统中定义 IPSec 安全策略来实现。一个 IPSec 安全策略由 IP 筛选器和筛选器操作两部分构成，其中 IP 筛选器决定哪些报文应当引起 IPSec 安全策略的关注，筛选器操作是指“允许”还是“拒绝”报文的通过。要新建一个 IPSec 安全策略，一般需要新建 IP 筛选器和筛选器操作。

基于 IP 的网络通信技术没有内建的安全机制。随着互联网的发展，安全问题逐渐暴露出来。现在经过各个方面的努力，标准的安全架构也已经基本形成。那就是 IPSec 机制，并且它将作为下一代 IP 网络标准 IPv6 的重要组成。IPSec 机制在新一代的操作系统中已经得到了很好的支持。在 Windows Server 2003 系统中，其服务器产品和客户端产品都提供了对 IPSec 的支持。从而增强了安全性、可伸缩性以及可用性，同时使部署和管理更加方便。在 Windows Server 2003 系统的安全策略相关的管理工具集(如本地安全策略、域安全策略、组策略等)中，都集成了相关的管理工具。用户可以根据情况来添加、修改和删除相应的 IP 安全策略。其中 Windows Server 2003 系统自带的策略如下。

(1) 采用 IPSec 加密数据通信的方法适用于企业网应用,通过部署组策略可以强制网络中的所有计算机使用 IPSec 加密通信。当然这种严格地限制会带来一些不便,不过对于系统安全来说是值得的。

(2) IPSec 还可以应用于 VPN 技术中,在这里可以对 IP 隧道中的数据流进行加密。对于不方便大范围实施 IPSec 的环境,可以考虑采用 VPN 技术。VPN 技术是目前实现端对端安全通信的最佳解决方案。

1.3.4 配置连接请求策略

对于企业网络,需要为一些远程拨号的用户提供拨号接入服务。远程拨号访问实际上是通过低速的拨号连接来将远程计算机接入到企业内部的局域网中。由于这个连接无法隐藏,因此常常成为黑客入侵内部网络的最佳入口。对于基于 Windows Server 2003 的远程访问服务器来说,默认情况下将允许具有拨入权限的所有用户建立连接。因此,安全防范的第一步就是合理地、严格地设置用户账户的拨入权限,严格限制拨入权限的分配范围,只要不是必要的就不给予此权限。对于网络中的一些特殊用户和固定的分支机构的用户来说,可通过回拨技术来提高网络安全性,这样就需要开通来电显示业务。

在 Windows Server 2003 网络中,如果活动目录工作在 Native-mode 下,这时就可以通过存储在访问服务器上或 Internet 验证服务器上的远程访问策略来管理。针对各种应用场景的不同,可以设置多种不同的策略。

1.3.5 防火墙策略

防火墙是网络安全的屏障。ISA Server 防火墙是建立在 Windows 操作系统上的一种可扩展的企业级防火墙,支持两个层级的策略:阵列级策略和企业级策略。

阵列级策略包括站点和内容规则、协议规则、IP 数据包筛选器、Web 发布规则和服务器发布规则。修改阵列配置时,该阵列内所有的 ISA Server 计算机也都会被修改,包括所有的访问策略和缓存策略。

企业级策略进一步体现了集中式管理,它允许设置一项或多项应用于企业网阵列的企业策略。企业级策略包括站点和内容规则,以及协议规则。企业级策略可用于任何阵列,而且可通过阵列自己的策略进行扩充。Windows Server 2003 支持 ISA Server 2000,但要安装补丁,为 ISA Server 升级。

1.3.6 组策略

Windows Server 2003 组策略和安全模板组策略用于从一个单独的点对多个 Microsoft Active Directory 目录服务用户和计算机对象进行配置。在默认情况下,策略不仅影响应用该策略的容器中的对象,还影响子容器中的对象。组策略包含了“计算机配置”→“Windows 设置”→“安全设置”下的安全设置。应用组策略可自动更新,但为了立即启动更新过程,可在命令提示符下使用 GPUpdate 命令,启用“安全配置和分析”。