高等职业教育“十一五”规划教材

高职高专市场营销类教材系列

网络安全与电子商务

CEAC信息化培训认证管理办公室 组编
章学拯 裘奋华 主编

CEAC
国家信息化计算机教育认证认证教材

科学出版社
www.sciencep.com

高等职业教育“十一五”规划教材

高职高专市场营销类教材系列

网络安全与电子商务

CEAC信息化培训认证管理办公室　组编

章学拯　裘奋华　主编

科学出版社

北　京

内 容 简 介

本书为高职高专市场营销类教材系列之一，也是 CEAC 信息化培训认证指定教材。

全书共分 10 章，主要包括电子商务安全的基础知识、信息加密技术与应用、数字签名技术与应用、数字证书与公钥基础设施、身份认证与访问控制、TCP/IP 与 WWW 安全、防火墙技术、计算机病毒及其防治技术、网络攻击与防御、电子商务应用安全解决方案等内容。

本书适合作为高职高专院校电子商务相关专业的教材，也可作为相关的培训教材。

图书在版编目(CIP)数据

网络安全与电子商务/CEAC 信息化培训认证管理办公室组编．—北京：科学出版社，2006

（高等职业教育“十一五”规划教材·高职高专市场营销类教材系列）

ISBN 7-03-017012-1

Ⅰ．网… Ⅱ．C… Ⅲ．①计算机网络-安全技术 ②电子商务

Ⅳ．①TP393.08 ②F713.36

中国版本图书馆 CIP 数据核字（2006）第 019489 号

责任编辑：丁 波 / 责任校对：都 岚

责任印制：吕春珉 / 封面设计：东方人华平面设计部

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

印刷

科学出版社发行 各地新华书店经销

*

2006 年 5 月第 一 版 开本：B5（720×1000）

2006 年 5 月第一次印刷 印张：19 1/2

印数：1—3 000 字数：390 000

定价：26.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

销售部电话 010-62136131 编辑部电话 010-62138978-8205（HF02）

前　言

随着 Internet 技术在商务领域应用的不断发展和普及，网络和信息安全的重要性日益突出。根据国家计算机网络应急技术处理协调中心（CNCERT/CC）的资料显示，2004 年 9～12 月 CNCERT/CC 收到的网络安全事件报告数量分别为 11535、14655、12532 和 9014 件，而这只是报告的数量，还没有包括更多的未报告的数量。在国内外电子商务应用与发展过程中，信息安全事例也不断出现，因此，电子商务的应用者也越来越重视其应用的安全问题。

各国政府和国内外相关机构与企业也在信息安全领域投入了巨资，用于研究和开发电子商务安全技术和解决方案。一些防病毒软件开发商现在基本上是每天提供多次升级服务，以应对不断出现的新病毒。Microsoft 公司的 Windows 操作系统等软件也是在不断地提供安全补丁。我国还专门建立了多个信息安全研究和产业基地，许多大学和科研机构都设立了信息安全研究部门。面对这种情况，各高校的相关专业也开设了信息安全的专门课程，譬如，各高校的电子商务专业都将电子商务安全纳入了本专业的主修课程，本书也是作者在电子商务专业讲授电子商务安全与认证课程的基础上编写而成的。

本书共分 10 章，主要内容如下：

第 1 章，讲述了电子商务安全的基础知识，包括电子商务概述和电子商务安全体系的内容。

第 2 章，讲述了信息加密技术及其应用，包括密码学的基本知识、对称与非对称密钥密码算法、单向加密算法和混和型加密体制等内容。

第 3 章，讲述了数字签名技术及其应用，包括数字签名的基本原理、数字签名算法和数字签名的应用等内容。

第 4 章，讲述了数字证书与公钥基础设施的相关知识，包括公钥基础设施的概念、公钥基础设施中的数字证书、公钥基础设施中密钥和证书的管理、公钥基础设施的相关标准等方面的内容。

第 5 章，讲述了身份认证与访问控制的知识，包括身份认证基础、身份认证协议、访问控制的概念和原理、访问控制的策略与机制等方面的内容。

第 6 章，讲述了 TCP/IP 与 WWW 安全方面的知识，包括 TCP/IP 基础、TCP/IP 协议的安全威胁及其解决方案、Web 的基本结构、Web 的安全保障等方面的内容。

第 7 章，讲述了防火墙的相关技术，包括防火墙的体系结构和防火墙产品介绍等方面的内容。

第 8 章，讲述了计算机病毒及其防治技术，包括计算机病毒机制、计算机病毒的防范、计算机病毒的发展趋势等方面的内容。

第 9 章，讲述了网络攻击与防御的知识，包括攻击者介绍、网络攻击、入侵的防御等方面的内容。

第 10 章，讲述了电子商务应用安全解决方案，包括 B to B 电子商务网站应用模式框架、B to B 电子商务网站的网络结构、B to B 电子商务网站的安全需求、B to B 电子商务网站的整体安全解决方案、WebST 应用于 B to B 电子商务、B to B 电子商务网站的安全服务过程等方面的内容。

本书由 CEAC 信息化培训认证管理办公室组编，上海对外贸易学院的章学拯和上海华东师范大学的裘奋华主编，其中，章学拯编写第 1～5、10 章，并负责全书框架结构的确定和统稿、审稿工作；裘奋华编写第 6～9 章。本书配有电子教案，有需要的读者请向我社索取。

由于编者水平有限，兼之时间仓促，书中难免有不妥之处，敬请广大读者批评指正。

目　录

第 1 章　电子商务安全基础知识

内容提要

电子商务的关键是商务信息的电子化。因此，电子商务安全的关键是电子信息的安全，即传递和处理商务信息的计算机网络及信息处理系统的安全。对计算机网络构成的安全威胁是多方面的。同样，可能实施的安全攻击具有多样性的特点。如何针对可能的安全威胁和攻击制定相应的安全策略和实施具体的安全机制是本章要介绍的重点内容。

本章学习目标

通过本章的学习应该了解和掌握以下内容:

① 电子商务安全的重要性。
② 黑客攻击网站的一般方法。
③ 电子商务安全的概念。
④ 电子商务安全的威胁及其分类。
⑤ 安全攻击及其分类。
⑥ 电子商务安全策略。
⑦ 电子商务安全机制与服务。
⑧ 电子商务安全管理。
⑨ 电子商务安全体系结构。

1.1　电子商务安全概述

2005 年 7 月 21 日，中国互联网络信息中心（CNNIC）在北京发布《第十六次中国互联网络发展状况统计报告》。报告显示，截至 2005 年 6 月 30 日，我国上网用户总数突破 1 亿，达 1.03 亿人。我国网上“购物大军”达到 2000 万人，网上支付的比例增长至近半数，网上购物市场巨大，网上购物者半年内累计购物金额达到 100 亿元，半年内通过网络购买的手机在 300 万部以上。同时有 26.9%的用户认为“网上购物存在的最大问题”是安全性得不到保障。

电子商务应用的快速发展促进了全球经济的发展。但随着电子商务交易规模的不断扩大，电子商务交易参与者的不断增加，电子商务安全问题的严峻性也日益突出。

1.1.1 电子商务安全典型案例

1、信用卡安全

就目前已经发现的盗窃信用卡账户信息的时间来看，至少存在以下 3 种窃取信用卡账户信息的手段。

（1）直接闯入存储信用卡账户信息的数据中心进行窃取

美国万事达信用卡国际公司 2005 年 6 月 17 日晚宣布，一名黑客侵入了“信用卡第三方付款处理器”（美国资讯厂商 CardSystems）的网络系统，可能造成包括万事达、Visa、American Express 和 Discover 在内的各种信用卡的高达 4000 多万用户的数据资料被窃，其中万事达信用卡用户高达 1390 万，Visa 信用卡的客户则高达 2200 万。专家称，这是到目前为止美国最大的泄密事件。

万事达国际公司称，这次遭遇泄露风险的主要是用户的姓名、银行和账户号码，而不是用户地址、生日、社会保障编号等其他信息，因此真正有被盗危险的是用户账户上的资金。

泄密是由于一种类似电脑病毒的脚本程序侵入电脑系统而发生的，这种程序可以用来捕获用户的重要资料，并利用这些资料进行金融犯罪。事件发生后，万事达公司通过声明表示，公司已经就此彻底要求 CardSystems 限期改善，立即修补安全漏洞。

美国资讯厂商 CardSystems 遭遇黑客入侵之事，并未过多波及我国持卡人。万事达信用卡国际公司表示，资料外泄并不意味着这些卡片会被盗用，持卡者的私人信息也不会外泄。此外，任何金融机构或者持卡者受到的损失，都将由 CardSystems 负责赔偿。

万事达国际公司表示，约有 5500 张在中国发行的万事达卡由于在美国使用过而受到影响，这些信用卡的持卡人在接到万事达国际公司通过国内相关银行的通知后，只能采取换卡的方式来防止信用卡被盗用。

（2）在用户计算机中植入木马程序，跟踪用户的击键过程进行窃取

据江民科技 2004 年 4 月 24 日报道：

4 月 24 日，江民反病毒专家警诫所有网上银行用户，虽然近期截获的“网银大盗”病毒专门盗取某网上银行的用户名和密码，但并不能排除其变种去盗取其他网上银行用户密码的可能，因为只需在技术上稍加改动，病毒就会将目标改成它愿意指向的任何一个目标。

4 月 19 日，江民反病毒中心接连截获“网银大盗”木马病毒及其变种，分析发现该病毒专门偷取某个网上银行的账号和密码，发送给病毒作者。

病毒运行后，将在用户计算机中创建可执行文件与挂钩和发信模块文件，并修改注册表，病毒在系统启动时即可运行。病毒主程序开启两个计时器，计时器

1 每隔 3 秒钟检查是否有常用反病毒和防火墙软件运行，一旦发现则立即终止这些进程，同时还自动回写病毒注册表项和病毒文件；计时器 2 每隔 0.5 秒钟搜索用户的浏览器窗口，如果发现用户正在“某网上银行”的登录界面，则尝试窃取注册卡号和密码。一旦成功，就把窃取到的信息保存到共享内存中，电脑与网络再次连通后，木马就会把共享内存中保存的用户账号和密码通过电子邮件的方式发送给病毒作者。

一个病毒出台后，其变种会紧跟着层出不穷，这也是 2004 年病毒发展的一个明显趋势，如网络天空病毒已出现二十几个变种，“网银大盗”及其变种也显现出了这种势头。

6 月 2 日，江民快速反病毒中心监测到，已于 4 月份被截获的“网银大盗”又出新变种。与上次“网银大盗”只盗取某网上银行用户号码不同的是，此次变种能突破大部分网上银行的安全防线，成功窃取用户账号和密码，网上银行潜在的资金威胁已上升到万亿级别！

江民病毒专家介绍，该病毒是一个 Key 记录程序，当它检测到用户在网上银行网页上进行支付或转账等操作时，就会记录当前的键盘输入，然后发送到病毒作者的服务器上。

（3）使用假冒银行网站的网页诱骗用户输入用户名和密码进行窃取

据《西安晚报》2004 年 12 月 10 日报道：

8 日，中国银行官方网站出现一条声明，该行目前唯一使用网址为：www.bank-of-china.com。据了解，是因为有人建了一个假冒的中国银行网站，试图骗取该行用户的账号和密码，该假冒网站已被公安部门查封。同时，记者还发现，有一个假冒的中国工商银行的网站 www.1cbc.com.cn 还在继续运行，它的网站和真正的中国工商银行网站 www.icbc.com.cn 只有“1”和“i”一字之差。

记者进入假中国工商银行网站 www.1cbc.com.cn 后，随便输入一个卡号并进行修改密码后，该网站显示“密码修改成功，请牢记”。专家介绍，如果此时输的是正确卡号和密码就已经被该网站盗取了。中国工商银行一位技术人员说，一旦犯罪分子掌握了他人的银行卡号和密码，就可以做假卡到提款机上取现金了。以前就有假中国工商银行网站出现，不过现在已被公安机关查封。

另据《深圳特区报》2005 年 2 月 16 日报道：

香港金融管理局（金管局）呼吁香港市民提高警觉，留意一个域名为“www.iivb.com”的怀疑欺诈网站。该网站声称由香港汇丰银行有限公司（汇丰银行）发送电子邮件，并向香港公众人士提供多项银行服务。

据了解，这个电子邮件载有一个可连接至欺诈网站的超链接，并要求客户经此网站输入网上理财户口的用户名称及密码，以核实其户口资料。该欺诈网站表面上

的设计与汇丰银行的个人网上理财网站的登录网站相似。汇丰银行2月16日向外澄清，并未向客户发出此类电子邮件，也未与该欺诈网站有关系。此外，汇丰银行并没有通过电子邮件要求客户提供其密码或在网上核实其户口资料这项政策。

图1-1所示为汇丰银行被假冒后，该行在网站上专门发布的安全提示。

图1-1 银行安全提示

以上案例暴露出了电子商务的安全隐患，那么如何消除这些安全隐患，保障电子商务安全呢？这就涉及到技术和法律两方面的问题。本书主要介绍电子商务安全的技术应用。

就技术而言，信用卡密码通常都使用加密技术加密后进行密文传输，所以企图盗窃用户密码的“盗贼”需要使用木马程序来跟踪用户的击键过程或使用假网页来骗取用户的账号和密码。针对窃贼使用木马程序和假网站窃取信用卡信息的伎俩，我们需要发展相应的安全技术来加以防范。

防范木马程序窃取信用卡信息的关键：一是不要轻易访问不明网站或下载和安装不明软件，以防止中毒；二是必须安装和及时更新防病毒软件，以便及时发现可能感染的病毒；三是在必须输入密码的时候，使用软键盘进行密码输入，以防止使用键盘输入时被跟踪。实际上大部分银行已经采取强制使用软键盘进行密码输入的措施（见图1-2）；四是必须安装防火墙软件，以防止木马程序对外发送窃取的消息。另外，有些木马程序是利用操作系统漏洞进行非法活动的，因此，及时升级操作系统，对可能存在的漏洞，安装补丁程序也是非常重要的。

在图1-2所示的界面中，银行还使用了要求输入“附加码”的策略，以防止不法之徒用程序自动填写密码的方法暴力破解信用卡密码。

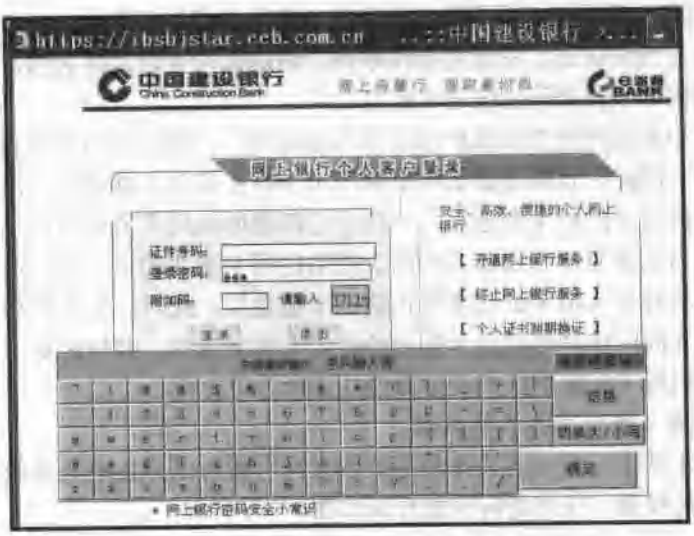

图 1-2　使用软键盘进行密码输入

防范假网站的关键：一是不要使用他人通过电子邮件或短信提供的银行网站地址，假冒网站通常使用形似真网站的地址，譬如，假中国工商银行网站使用 www.1cbc.com.cn 来假冒中国工商银行网站的地址（www.icbc.com.cn）；二是在进行账户登录前，双击网页下方的安全锁，检查网站的数字证书（见图 1-3），真实的银行网站都使用用于确认网站身份的数字证书，并使用证书所包涵的密钥进行信息加密。

图 1-3　检查网站的数字证书

由此可见，银行和信用卡持卡人在保护信用卡信息的安全方面已经采取了使用数据加密、身份认证、安全的操作系统、防病毒软件以及防火墙，并且使用软键盘和附加码等手段来保护信用卡信息。

持卡人如果选择用密码保护信用卡不被盗用，在使用信用卡消费或提款时均须输入密码。因此，及时变更信用卡密码可以防止信用卡被盗用。但在不需要密码即可使用信用卡的国家和地区，要防止已泄密的信用卡被盗用的唯一方法是换卡。然而作为电子商务主要模式的网上使用信用卡消费的话，我们通常是使用与信用卡配套的持卡人数字证书来防止信用卡被盗用。此时，发卡机构在发卡的同时要求持卡人同时申请与信用卡配套的持卡人数字证书，并规定对于一些重要的操作必须使用持卡人数字证书经过身份认证后方可进行。

2. 攻击者攻击计算机系统流程

如图 1-4 所示，攻击者攻击服务器的过程一般可以分为进入系统、提升或获取系统管理员权限、保持访问和离开四部曲。

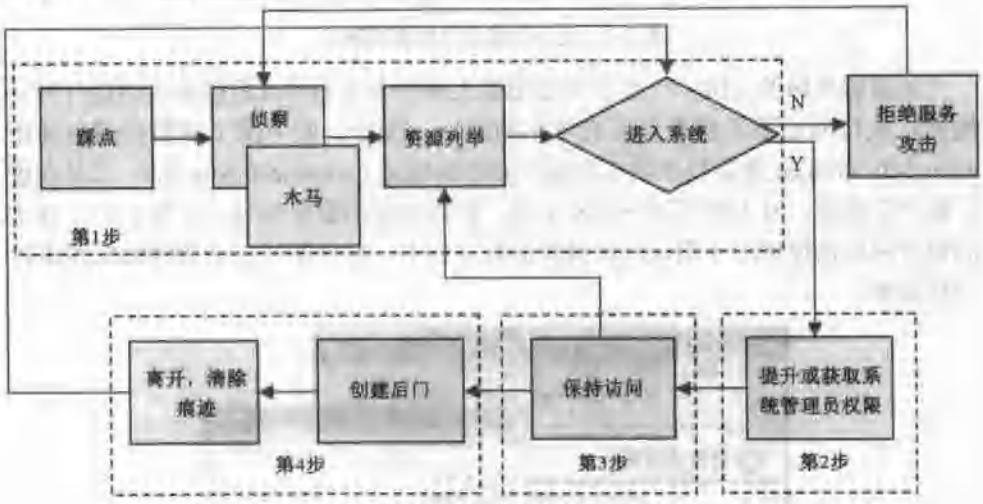

图 1-4 攻击服务器的过程

（1）进入系统

黑客进入一个新的攻击对象要经过踩点、侦察、资源列举等几个步骤。在病毒流行的今天，更有攻击者利用木马病毒直接控制被攻击对象的计算机系统。

1）踩点。踩点就是通过各种途径对要攻击的目标进行多方面的了解（包括任何可得到的蛛丝马迹，但要确保信息的准确）。

踩点的内容包括域名及其注册机构的查询、公司性质的了解、对主页进行分析、邮件地址的搜集以及目标 IP 地址范围查询。查询对方 IP 地址的方法很多，可以使用专门软件、防火墙软件或 DOS 命令进行查询。