新概念教材

中国高等院校市场学研究会
中国高等职业技术教育研究会电子商务与物流协作委员会 规划组编

高职高专教育电子商务专业教材新系

电子商务安全技术

劳帼龄 主编

东北财经大学出版社
Dongbei University of Finance & Economics Press

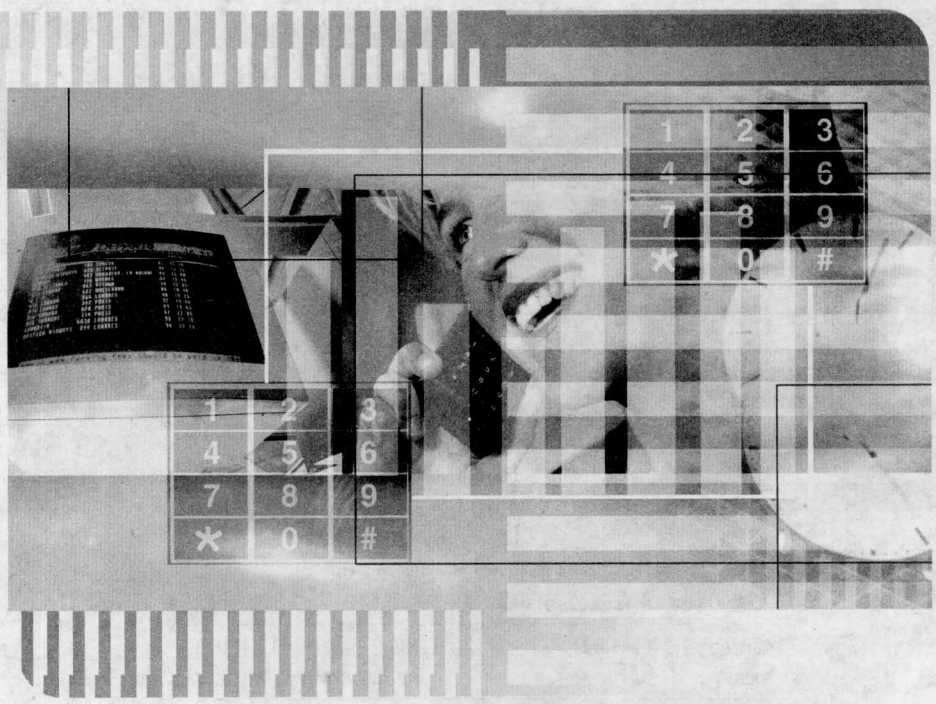
新概念教材

中国高等院校市场学研究会
中国高等职业技术教育研究会电子商务与物流协作委员会 规划组编

高职高专教育电子商务专业教材新系

电子商务安全技术

劳帼龄 主编



东北财经大学出版社
Dongbei University of Finance & Economics Press
大 连

图书在版编目（CIP）数据

电子商务安全技术 / 劳帼龄主编 . —大连 ： 东北财经大学出版社，2008. 5
（高职高专教育电子商务专业教材新系）
ISBN 978 - 7 - 81122 - 344 - 6

Ⅰ. 电… Ⅱ. 劳… Ⅲ. 电子商务 - 安全技术 - 高等学校：技术学校 - 教材 Ⅳ. F713. 36

中国版本图书馆 CIP 数据核字（2008）第 062990 号

东北财经大学出版社出版
（大连市黑石礁尖山街 217 号 邮政编码 116025）
总 编 室：（0411）84710523
营 销 部：（0411）84710711
网 址：http：//www. dufep. cn
读者信箱：dufep @ dufe. edu. cn
大连力佳印务有限公司印刷 东北财经大学出版社发行

幅面尺寸：170mm × 240mm 字数：386 千字 印张：16 3/4
2008 年 5 月第 1 版 2008 年 5 月第 1 次印刷

责任编辑：许景行 龚小晖 责任校对：赵 楠
封面设计：张智波 版式设计：钟福建

ISBN 978 - 7 - 81122 - 344 - 6
定价：29. 00 元

总　　序

电子商务是发展迅猛的新兴产业。在我国，电子商务历史虽短，但从20世纪90年代初的EDI电子商务应用，到其后的“三金工程”，再到90年代末开始的互联网，发展势头极为强劲。进入21世纪，电子商务带动了企业管理与商务模式的创新，对经济环境与国际政策的挑战也日益显著，特别是对于中小企业，电子商务发展的潜力不可估量。

与产业发展同步，电子商务专业是我国多数高等院校开设的大专业之一。迄今为止，在全国1 100所高职院校中，已有700多所开设了电子商务专业，为社会源源不断地提供大量电子商务高等应用型人才。

在专业课程设置方面，国内高职院校经过近几年教学计划的交流，并借鉴国外特别是欧美电子商务教育经验，已在主要方面达成阶段性共识，提炼出以网络技术与应用、数据库技术与应用和网页设计与制作等技术基础课为依托，以电子商务概论、电子商务网站建设与维护、电子商务安全管理、网络营销、电子商务法律、网络编辑、电子商务英语、电子商务综合实训等专业课为主干，以国际贸易实务、电子商务项目管理、客户关系管理、电子商务物流等拓展课为补充的高职高专电子商务专业课程体系。

根据上述新的课程体系设计推出的“21世纪新概念教材·高职高专教育电子商务专业教材新系”（共15种），由中国高等院校市场学研究会和中国高等职业技术教育研究会电子商务与物流协作委员会（以下简称“两会”）规划组编，东北财经大学出版社出版，其领衔作者是从全国各高校专业带头人中择优遴选出来的，他们或者是国家精品课程的主讲者，或者是本专业领域的资深专家。

本套教材具有六大鲜明特色：

1. 与时俱进的课程设置：与国内外高校电子商务专业教学改革新进展保持同步。

2. 合理先进的代型设计：定位于“产学研结合”，着眼于“双证沟通”，涉足于“创新教育”，突出“高等应用性”，充分展示既定成果，也适当关注“问题意识”。

3. 能力本位的人才模式：坚持整合论意义上的“知识教育、技能训练和能力培养三者统一”。

4. 简明优化的教学内容：按照“先进、精简、适用”的原则对教学内容进行优化重组。

5. 典型到位的案例穿插：章首的“引例”，节内的“微型案例”，章后的“中型案例”与书后的“综合案例”融为一体。

6. 系统完备的教辅支持：免费提供网络教辅系列，“PPT教学课件”、“章后习题参考答案与提示”、“综合案例分析提示”、“综合实训教学建议”、“综合讨论参考资料”、“试题题库”等一应俱全。

作为全国通用的最新教学用书，本套教材是高等职业技术院校、高等专科学校、本科

院校二级学院、五年制高职等电子商务专业、IT 专业、工商管理专业及其他财经类相关专业的首选，也可供成人高校、电大、民办高校和社会从业人员参考使用。

本套教材只是“两会”高职教育教学改革与创新研究的阶段性成果，这些成果在取得上述突破的同时，尚存在某些方面的不足。这些不足的克服，有赖于在广大专家和读者支持与关怀下的不断修订。

“高职高专教育电子商务专业教材新系”

编写委员会

编审说明

本书是全国高职高专教育通用教材，经审定，同意将其作为“两会”规划教材出版。书中不当之处，欢迎读者批评指正。

中国高等院校市场学研究会
中国高等职业技术教育研究会电子商务与物流协作委员会
规划教材审定组

前　言

电子商务从20世纪90年代中期诞生以来，已经走过了十余年的发展历程。十几年来，安全问题始终是影响其发展的一个瓶颈。这在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中可见一斑，历次调查，安全问题一直是电子商务用户特别关注的主题。可以说，电子商务安全是电子商务顺利发展的一个关键，也是一个难点。

大量的事实说明，要保证电子商务的正常运作，就必须要高度重视电子商务的安全问题。电子商务的安全涉及社会的方方面面，不是一堵防火墙或一个电子签名就能简单解决的问题。安全问题既是电子商务成功与否的关键所在，也是致命所在。因为电子商务的安全问题不仅关系到个人的资金安全、商家的货物安全、企业的交易安全，还关系到国家的经济安全，关系到国家经济秩序的稳定问题。而要保障电子商务的安全，除了要充分依靠现代信息技术，尤其是信息安全技术手段来进行保护外，还需要安全管理的制度和手段来约束，需要法律、法规环境的保障。

本书由8章组成。第1章电子商务安全概述，首先引出电子商务面临的安全问题，介绍电子商务安全的概念与基本要求、电子商务安全的保障，以及电子商务安全的未来工作。第2章信息加密技术，主要介绍网络通信中的加密方式、分组加密与高级加密标准、公开密钥加密体制、复合型加密体制PGP，以及非密码的安全技术。第3章数字签名技术与应用，主要介绍数字签名的基本原理、常规数字签名方法、特殊数字签名方法，以及美国数字签名标准。第4章数字证书，先简要介绍什么是数字证书，随后介绍数字证书的格式、数字证书的申请与发放、数字证书的分发、数字证书的撤销/吊销，最后介绍了个人数字证书在电子邮件中的应用。第5章公钥基础设施PKI，首先概要介绍什么是PKI，随后介绍PKI的核心——CA，以及PKI的实施和基于PKI的电子商务交易系统。第6章网络安全技术，主要介绍网络安全的基本概念、WWW的安全性问题、防火墙技术、VPN技术，以及网络入侵检测技术。第7章计算机病毒及其防范，主要介绍计算机病毒的基本概念、计算机病毒的防范，以及网络病毒的防范。第8章系统评估准则与安全策略，主要介绍系统评估准则、信息安全测评认证准则、安全管理的实施、安全策略的制定、系统备份和紧急恢复的方法、审计与评估，以及容灾技术及其典型应用。

考虑到高职高专教育的特点，本书注重了“知识”、“技能”和“能力”的结合。每章开头清楚地列明本章的知识目标、技能目标和能力目标，让读者一目了然。然后用一个小案例引发读者的思考，带出本章要介绍的内容。每章结尾都对本章内容进行分析评价和小结，以帮助读者掌握本章要点。最后，用主要概念和观念的复习，由简答、选择、阅读理解、技术应用构成的知识训练，及单项操作和综合操作构成的技能训练，以及由案例、实训、讨论构成的观念应用，三管齐下帮助读者通过练习来检验对本章内容的掌握情况。

在8章内容全部介绍完毕后，给出了综合案例分析、综合实训以及综合讨论，检验读者对知识技能的综合掌握和应用情况。

为方便教学，我们为本教材提供了丰富的网上教学资源，即电子教学课件和6个“附录”。这6个“附录”是：“章后习题参考答案与提示”、“综合案例分析提示”、“综合实训教学建议”、“综合讨论参考资料”、“试题题库”和“试题题库参考答案与提示”。使用本教材的教师可登录东北财经大学出版社网站（www. dufep. cn）查询或下载这些教学资源。

本书由劳帼龄主编。参与本书资料收集和编写工作的还有钟艳萍、兴磊、何雪鹃、胡人可、刘灿进、杨凯。

本书在编写过程中，大量参考和借鉴了国内外有关电子商务安全技术的著作、教材、文章和网站资料，吸收了前人的研究成果，在此一并表示感谢。尽管在本书的编写工作中，作者努力想把与电子商务安全相关的最新知识介绍给读者，但限于水平和经验，加上电子商务本身的发展迅速，书中疏漏之处在所难免，敬请广大读者批评指正。

劳帼龄

2008年4月

目　录

第1章

电子商务安全概述

■ 学习目标

知识目标：

了解电子商务安全的概念；了解电子商务系统安全的构成；理解电子商务安全保障基本原则的实质意义。

技能目标：

依据电子商务安全的基本内容与特点，掌握电子商务安全的需求；掌握电子商务安全保障的基本原则。

能力目标：

能够灵活应用辨别电子商务安全问题的能力，能根据电子商务安全保障的要求指导行动。

引例：电子商务发展的主要障碍是什么

随着互联网的全面普及，基于互联网的电子商务也应运而生，并在近年来获得了巨大的发展，成为一种全新的商务模式，被许多经济专家认为是新的经济增长点。

作为一种全新的商务模式，它有很大的发展前途，同时，这种电子商务模式对管理水平、信息传递技术都提出了更高的要求，其中安全体系的构建又显得尤为重要。如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，是商家和用户都十分关注的话题。安全问题已成为电子商务的核心问题。

联合国贸易与发展会议2005年11月发布了《2005年信息经济报告——电子商务与发展》，该报告称："到2002年年底，全球互联网用户人数达到6.55亿，比上年同期增长了30%；网上商品和服务的销售量达到23亿美元，比上年同期增长了50%。到2003年，这个数字将增长39亿美元。"

这篇报告指出："按照目前的增长率，到2006年，企业和个人购买的全部商品将有18%是在网上购买的。"

但是，电子商务贸易额在全球贸易额中仍只占一小部分。例如，1997年美国的整个贸易额为25 200亿美元，而2001年的电子商务贸易额为3 270亿美元，还不到1997年美国两个月的贸易额。

资料来源　佚名：《联合国贸发会议发表〈2005年电子商务报告〉》，genevese. mofcom. gov. cn/aarticle/ddfg/haiguan/200512/20051201087747. html。

人们不禁要问，是什么因素阻碍了电子商务的普及呢？为此，不少调查机构进行了广泛的调查，从众多的调查中发现，一个主要的障碍就是电子商务的安全问题。美国密执安大学一个调查机构通过对23 000名因特网用户的调查显示，超过60%的人由于担心电子商务安全问题而不愿意进行网上购物。

的确，由于因特网的全球性、开放性、无缝连通性、共享性和动态发展使得任何人都可以自由地介入因特网，特别是黑客们可能会采用各种攻击手段进行破坏等犯罪活动。此外，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。另外，由于金钱和财富的利诱，大大刺激了黑客们以身试法。因此，在建立电子商务应用系统时，必须将安全作为一个重要方面来加以考虑。

1.1　电子商务面临的安全问题

1.1.1　安全问题的提出

任何技术的发展都有其正反两方面的效应，电子商务也不例外，它在带给人们方便、快捷、廉价、高效的商务活动的同时，也给使用者带来相当多的安全问题。

1）商家面临的安全问题

①中央系统安全性被破坏。入侵者假冒合法用户来改变用户数据（如商品送达地址）、解除用户订单或生成虚假订单。

②竞争者检索商品的销售情况。恶意的竞争者以他人名义来订购商品，从而了解有关商品的递送状况和货物的库存情况。

③客户资料被竞争者获悉。

④被他人冒名而损害企业的名誉。

⑤消费者提交订单后不付款。

2）客户所面临的安全问题

①虚假订单。假冒者可能会用另一个客户的名字来订购商品，而且有可能收到商品，而被假冒的客户却被要求付款或返还商品。

②付款后收不到商品。

③机密性丧失。客户可能将秘密的个人数据或自己的身份数据（如 Pin 口令等）发送给冒名为销售商的机构。同时，这些信息在传递的过程中也有可能受到被窃听的威胁。

④拒绝服务。攻击者可能向销售商的服务器发送大量的虚假订单来挤占它的资源，从而使合法的用户得不到正常的服务。

3）银行专用网络所面临的安全问题

电子商务活动中的安全风险，还有很大一部分来自于攻击者对银行专用网络的破坏。攻击者破坏银行专用网络所采用的手段大致有以下 4 类：

①中断（攻击系统的可用性），即破坏银行专用网络系统中的硬件、线路、文件系统等，使系统不能正常工作。

②窃听（攻击系统的机密性），即通过搭线与电磁泄漏等手段造成泄密，或对银行专用网络中的业务流量进行分析，获取有用情报。

③篡改（攻击系统的完整性），即篡改银行专用网络中的数据内容，修改消息次序、时间（延时和重放）等。

④伪造（攻击系统的真实性），即将伪造的虚假消息输入银行专用网络、冒名合法人员介入银行专用网络、重放截获的合法消息以实现非法目的、否认消息的接收和发送等。

1.1.2 安全漏洞

根据国际权威应急组织 CERT/CC 统计，2005 年全年收到漏洞报告 5 990 个，平均每天超过 15 个。自 1995 年以来共计收到漏洞报告 22 716 个，具体结果如图 1—1 所示。漏洞的大量存在是电子商务安全问题的总体形势趋于严峻的重要原因之一。

1.1.3 病毒感染

我国计算机病毒感染率自 2001 年以来就一直处于较高的水平。2004 年，蠕虫等病毒在网上传播仍十分猖獗，计算机感染率从 2001 年的 73% 跃到了 2004 年的 87.93%。蠕虫病毒主要是利用系统的漏洞进行自动传播复制，由于传播过程中产生巨大的扫描或其他攻击流量，从而使网络流量急剧上升，造成网络访问速度变慢甚至瘫痪，这对依赖于网络的电子商务是一个严重的威胁。

2004 年没有爆发对整个网络运行安全造成重大影响的蠕虫等病毒事件，而主要是造成大量用户无法正常使用。尽管如此，蠕虫等病毒传播对局部网络造成的影响仍是不容乐观的。2004 年以来蠕虫病毒出现了一些新特点。蠕虫病毒被黑客用来驱动预定的拒绝服务攻击，如冲击波、Mydoom 蠕虫等，如果这种方法被应用于对互联网上的关键节点服务器、路由器进行拒绝服务攻击，将会导致整个互联网业务的瘫痪，且在理论上，并没有有效的方法来应对该类攻击。蠕虫病毒也逐渐被用来植入木马程序和后门软件，如“震荡波”系列蠕虫等，给感染蠕虫病毒的用户带来严重的泄密威胁，同时也造成大量潜在的

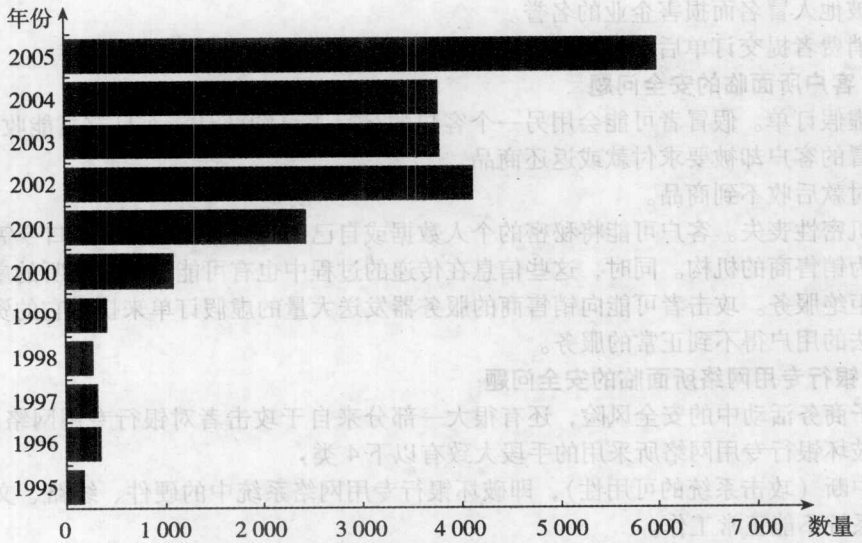


图 1—1 1995—2005 年漏洞公布数量

可受黑客控制的主机，一旦某个黑客或黑客组织集中控制了这些主机，将给各种网络应用系统带来不堪设想的严重威胁。

【小资料 1—1】

教你怎样用安全网关消灭蠕虫病毒

自 1988 年出现第一个蠕虫病毒以来，计算机蠕虫病毒以其快速、多样化的传播方式不断给网络世界带来灾害。蠕虫病毒不同于一般的病毒，它以计算机为载体，复制自身在互联网环境下进行传播。魔高一尺，道高一丈，随着蠕虫病毒的快速演变，解毒的高手也不断涌现。

首先是检测，这一步骤需要手工来操作。网络中的蠕虫病毒不断向外界计算机发出扫描包，这些扫描包是有明显特点的。例如，被感染的计算机中的蠕虫病毒会向网络中的某段 IP 地址发送扫描包。由于网络所发送、接收的包都要经过路由器，而通过路由器的 Web 管理界面就可以轻松看到。所以，蠕虫病毒攻击的特点反映在上网监控页面上就是：感染的主机发出大量的 NAT 会话，会话中只有上传包，下载包很小或者为零。如果存在这样的主机，说明该主机已经被蠕虫病毒感染。

这种情况下，就要进入第二步，即对网络中的主机实施屏蔽。屏蔽的方法是：利用路由器的管理功能制定相应的策略，关闭病毒向外发包的端口，采取杀毒措施或者安装相应的补丁程序。这样，就可以轻松消灭蠕虫病毒。

资料来源 www. hacker. com. cn/article/list. asp? id = 3343.

1.1.4 黑客攻击

1）网页篡改

从 2001 年日本前首相小泉纯一郎参拜靖国神社以来，该神社的网页就断断续续遭到黑客的攻击，有时在 1 分钟内就遭到 90 万次围攻；2004 年 10 月末，黑客入侵负责托管巴

西所有政府网站的互联网服务供应商，在200多个巴西政府网站上留下了反政府言论；2004年10月28日，索尼（中国）有限公司的网页被篡改，加入了辱骂美国总统布什的话语，并对其发动的伊拉克战争进行了抨击；2004年12月25日和27日麦当劳中文官方网站三次被黑客篡改，或是将主页颜色更改，添加抗议麦当劳把台湾从中国分裂出去的标语，或是用简单的页面替换掉麦当劳主页。当月29日，耐克中文网站也被黑客篡改，如图1—2所示。

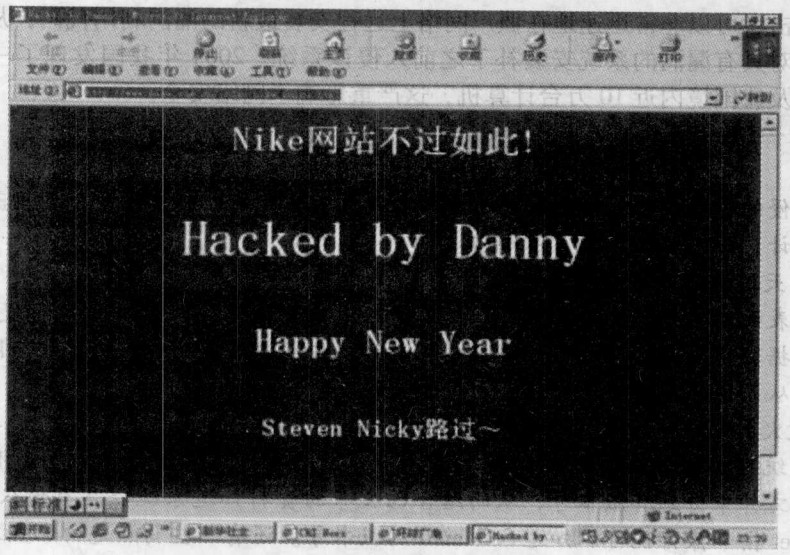


图1—2　耐克中文网站被黑客篡改

面对频繁的网页篡改事件，黑客们表示，他们并非为中国而来，只是想告诉全世界，“You don't have security”。从图1—3的网页篡改情况统计可以看出，网页篡改事件频繁发生，平均每天发生6起。

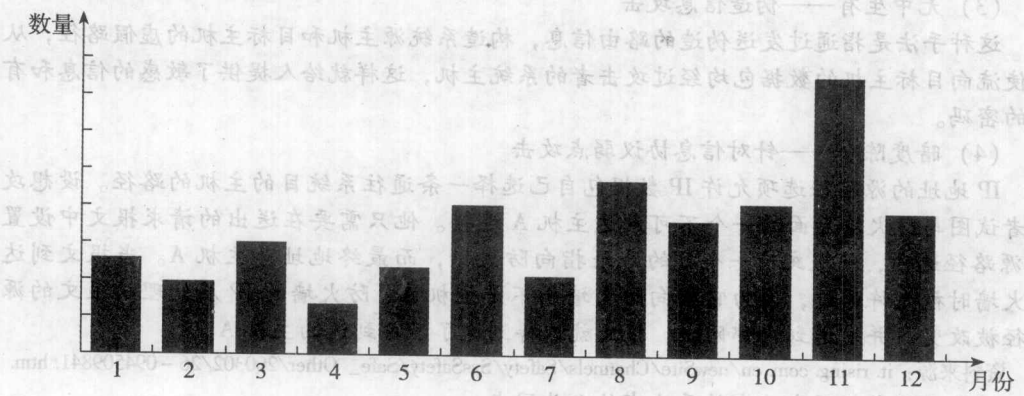


图1—3　2004年中国内地网页篡改情况

2）僵尸网络

僵尸网络也称为BotNet，Bot是robot的简写，通常是指可以自动执行预定义的功能，

可以被预定义的命令控制，具有一定人工智能的程序。它可以通过溢出漏洞攻击、蠕虫邮件、网络共享、口令猜测、P2P 软件等途径进入用户主机。一旦用户主机被植入 Bot，就主动和互联网上的一台或多台控制节点取得联系，进而自动接收黑客通过这些控制节点发送的控制命令，这些受害主机和控制服务器就组成了 BotNet。

2004 年的前六个月中，所监控的 bot 的平均数目从每天不到 2 000 个增加到每天 30 000个以上，高峰时一天可达到 75 000 个。僵尸网络为各个企业/机构带来了特有的问题：由于攻击者可以非常迅速地在僵尸网络上远程安装最新的漏洞利用代码，从而可能赶在一个机构对具有漏洞的系统安装补丁之前入侵该系统。2004 年我国发现了一个大型僵尸网络，涉及我国境内近 10 万台计算机，这严重影响了网络安全。

【观念应用 1—1】

黑客入侵计中计

黑客入侵的手法包括：瞒天过海、趁火打劫、无中生有、暗度陈仓、笑里藏刀等，黑客常有连环计，防不胜防，不可不小心。

（1）瞒天过海——数据驱动攻击

当有些表面看来无害的特殊程序在被发送或复制到网络主机上并被执行发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以造成一台主机修改与网络安全有关的文件，从而使黑客下一次更容易入侵该系统。

（2）趁火打劫——系统文件非法利用

Unix 系统可执行文件的目录，如/bin/who 可由所有的用户进行读访问。有些用户可以从可执行文件中得到其版本号，从而结合已公布的资料知道系统会具有什么样的漏洞，如通过 Telnet 指令操行就可以知道 Sendmail 的版本号。还有一些弱点是由配置文件、访问控制文件和缺省初始化文件产生的。最典型的一个例子是用来安装 SunOS Version 4 的软件，它创建了一个 rhosts 文件，这个文件允许局域网（因特网）上的任何人，从任何地方取得对该主机的超级用户特权。当然，最初这个文件的设置是为了从网上方便地进行安装，而不需超级用户的允许和检查。

（3）无中生有——伪造信息攻击

这种手法是指通过发送伪造的路由信息，构造系统源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的系统主机，这样就给人提供了敏感的信息和有用的密码。

（4）暗度陈仓——针对信息协议弱点攻击

IP 地址的源路径选项允许 IP 数据包自己选择一条通往系统目的主机的路径。设想攻击者试图与防火墙后面的一个不可到达主机 A 连接。他只需要在送出的请求报文中设置 IP 源路径选项，使报文有一个目的地址指向防火墙，而最终地址是主机 A。当报文到达防火墙时被允许通过，因为它指向防火墙而不是主机 A。防火墙的 IP 层处理该报文的源路径被改变，并发送到内部网上，报文就这样到达了不可到达的主机 A。

资料来源：it. rising. com. cn/newSite/Channels/Safety/SysSafety/Safe_ Other/200302/26 - 094509841. htm.

问题：试分析黑客攻击的手法有什么共同点。

1.1.5 网络仿冒

2004 年 12 月 8 日，中国银行发现，有一个网址为“www. bank - off - china. com”的