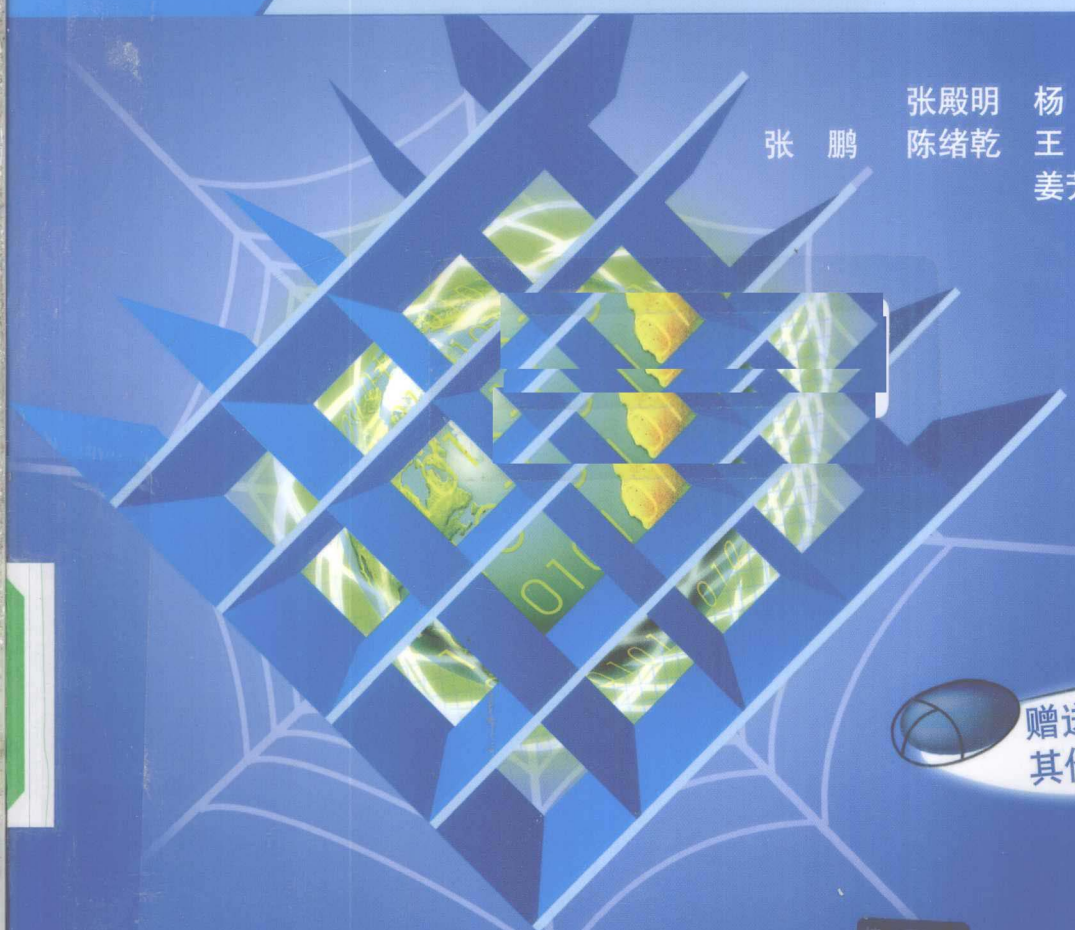
高职高专立体化教材计算机系列

计算机网络安全

JISUANJI WANGLUO ANQUAN

张殿明 杨 辉 主 编
张 鹏 陈绪乾 王 妍 副主编
姜芳艽 主 审



赠送电子课件及
其他立体化资源

清华大学出版社

高职高专立体化教材　计算机系列

计算机网络安全

张殿明　杨　辉　主　编
张　鹏　陈绪乾　王　妍　副主编
姜芳艽　主　审

清华大学出版社
北　京

内 容 简 介

本书从网络安全的角度出发，全面介绍网络安全的基本理论以及网络安全方面的管理、配置和维护。全书共分9章，主要内容包括网络安全概述、网络攻击与防范、拒绝服务与数据库安全、计算机病毒与木马、安全防护与入侵检测、加密技术与虚拟专用网、防火墙、网络应用服务安全配置和无线网络安全。各章后都编排了习题，供学生课后复习与巩固所学知识。

本书注重实习性，实例丰富、典型，实验内容和案例融合在课程内容中，将理论知识与实践操作很好地结合起来。

通过本书的学习，读者可以对网络安全有一个全面而系统的认识，同时可以学会使用网络安全工具。本书可作为高职高专计算机、网络技术、电子商务等相关专业学生的教材，也可供相关技术人员作为参考书或培训教材。

图书在版编目(CIP)数据

计算机网络安全/张殿明，杨辉主编；张鹏，陈绪乾，王妍副主编；姜芳艽主审. —北京：清华大学出版社，2010.4
(高职高专立体化教材　计算机系列)
ISBN 978-7-302-21960-6
Ⅰ. 计…　Ⅱ. ①张…　②杨…　③张…　④陈…　⑤王…　⑥姜…　Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2010)第 018603 号

责任编辑：石　伟
封面设计：山鹰工作室
版式设计：杨玉兰
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**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
印 刷 者：北京市昌平环球印刷厂
装 订 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.25　**字　数**：464 千字
版　　次：2010 年 4 月第 1 版　　**印　　次**：2010 年 4 月第1 次印刷
印　　数：1～4000
定　　价：29.00 元

产品编号：031928-01

《高职高专立体化教材计算机系列》

丛 书 序

一、编写目的

关于立体化教材，国内外有多种说法，有的叫“立体化教材”，有的叫“一体化教材”，有的叫“多元化教材”，其目的是一样的，就是要为学校提供一种教学资源的整体解决方案，最大限度地满足教学需要，满足教育市场需求，促进教学改革。我们这里所讲的立体化教材，其内容、形式、服务都是建立在当前技术水平和条件基础上的。

立体化教材是一个“一揽子”式的，包括主教材、教师参考书、学习指导书、试题库在内的完整体系。主教材讲究的是“精品”意识，既要具备指导性和示范性，也要具有一定的适用性，喜新不厌旧。那种内容越编越多，本子越编越厚的低水平重复建设在“立体化”的世界中将被扫地出门。和以往不同，“立体化教材”中的教师参考书可不是千人一面的，教师参考书不只是提供答案和注释，而是含有与主教材配套的大量参考资料，使得老师在教学中能做到“个性化教学”。学习指导书更像一本明晰的地图册，难点、重点、学习方法一目了然。试题库或习题集则要完成对教学效果进行测试与评价的任务。这些组成部分采用不同的编写方式，把教材的精华从各个角度呈现给师生，既有重复、强调，又有交叉和补充，相互配合，形成一个教学资源有机的整体。

除了内容上的扩充，立体化教材的最大突破还在于在表现形式上走出了“书本”这一平面媒介的局限，如果说音像制品让平面书本实现了第一次“突围”，那么电子和网络技术的大量运用就让躺在书桌上的教材真正“活”了起来。用 PowerPoint 开发的电子教案不仅大大减少了教师案头备课的时间，而且也让学生的课后复习更加有的放矢。电子图书通过数字化使得教材的内容得以无限扩张，使平面教材更能发挥其提纲挈领的作用。

CAI 课件把动画、仿真等技术引入了课堂，让课程的难点和重点一目了然，通过生动的表达方式达到深入浅出的目的。在科学指标体系控制之下的试题库既可以轻而易举地制作标准化试卷，也能让学生进行模拟实战的在线测试，提高了教学质量评价的客观性和及时性。网络课程更厉害，它使教学突破了空间和时间的限制，彻底发挥了立体化教材本身的潜力，轻轻敲击几下键盘，你就能在任何时候得到有关课程的全部信息。

最后还有资料库，它把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，大大方便了教师在备课、开发电子教案和网络课程时的教学工作。如此一来，教材就“活”了。学生和书本之间的关系不再像领导与被领导那样呆板，而是真正有了互动。教材不再只为教师们规定什么重要什么不重要，而是成为教师实现其教学理念的最佳拍档。在建设观念上，从提供和出版单一纸质教材转向提供和出版较完整的教学解决方案；在建设目标上，以最大限度满足教学要求为根本出发点；在建设方式上，不单纯以现有教材为核心，简单地配套电子音像出版物，而是

以课程为核心，整合已有资源并聚拢新资源。

网络化、立体化教材的出版是我社下一阶段教材建设的重中之重，作为以计算机教材出版为龙头的清华大学出版社确立了“改变思想观念，调整工作模式，构建立体化教材体系，大幅度提高教材服务”的发展目标。并提出了首先以建设“高职高专计算机立体化教材”为重点的教材出版规划，希望通过邀请全国范围内的高职高专院校的优秀教师，在2008年共同策划、编写这一套高职高专立体化教材，利用网络等现代技术手段实现课程立体化教材的资源共享，解决国内教材建设工作中存在教材内容的更新滞后于学科发展的状况。把各种相互作用、相互联系的媒体和资源有机地整合起来，形成立体化教材，把教学资料以知识点为单位，通过文字、图形、图像、音频、视频、动画等各种形式，按科学的存储策略组织起来，为高职高专教学提供一整套解决方案。

二、教材特点

在编写思想上，以适应高职高专教学改革的需要为目标，以企业需求为导向，充分吸收国外经典教材及国内优秀教材的优点，结合中国高校计算机教育的教学现状，打造立体化精品教材。

在内容安排上，充分体现先进性、科学性和实用性，尽可能选取最新、最实用的技术，并依照学生接受知识的一般规律，通过设计详细的可实施的项目化案例(而不仅仅是功能性的小例子)，帮助学生掌握要求的知识点。

在教材形式上，利用网络等现代技术手段实现立体化的资源共享，为教材创建专门的网站，并提供题库、素材、录像、CAI 课件、案例分析，实现教师和学生在更大范围内的教与学互动，及时解决教学过程中遇到的问题。

本系列教材采用案例式的教学方法，以实际应用为主，理论够用为度。教程中每一个知识点的结构模式为“案例(任务)提出→案例关键点分析→具体操作步骤→相关知识(技术)介绍(理论总结、功能介绍、方法和技巧等)”。

本系列教材将提供全方位、立体化的服务。网上提供电子教案、文字或图片素材、源代码、在线题库、模拟试卷、习题答案、案例动画演示、专题拓展、教学指导方案等。

在为教学服务方面，主要是通过教学服务专用网站在网络上为教师和学生提供交流的场所，每个学科、每门课程，甚至每本教材都建立网络上的交流环境。可以为广大教师信息交流、学术讨论、专家咨询提供服务，也可以让教师发表对教材建设的意见，甚至通过网络授课。对学生来说，则可以在教学支撑平台上所提供的自主学习空间上来实现学习、答疑、作业、讨论和测试，当然也可以对教材建设提出意见。这样，在编辑、作者、专家、教师、学生之间建立起一个以课本为依据、以网络为纽带、以数据库为基础、以网站为门户的立体化教材建设与实践的体系，用快捷的信息反馈机制和优质的教学服务促进教学改革。

本系列教材专题网站：http://www.wenyuan.com.cn。

前　言

计算机网络安全已引起世界各国的关注，我国近几年才逐渐开始在高等教育中渗透计算机网络安全方面的基础知识和网络安全技术应用知识。随着网络高新技术的不断发展，社会经济建设与发展越来越依赖于计算机网络。与此同时，网络中不安全因素对国民经济的威胁，甚至对国家和地区的威胁也日益严重。加快培养网络安全方面的应用型人才、广泛普及网络安全知识和掌握网络安全技术就突显重要和迫在眉睫。但是，这方面的著作，特别是适合高职院校的著作极为缺乏。本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的网络攻防技术实例，并通过研究实践而形成的一本高职高专计算机及相关专业网络安全课程的教材，全书系统而全面地介绍了网络安全与管理方面的相关内容，在每章的最后安排了实训内容，旨在使读者能够综合运用书中所讲授的知识进行网络安全与管理方面的实践。

本书更注重以能力为中心，以培养应用型和技能型人才为根本，通过认识、实践、总结和提高这样一个认知过程，精心组织学习内容，图文并茂、深入浅出，全面适应社会发展需要，符合高等职业教育教学改革规律及发展趋势，具有独创性、层次性、先进性和实用性。全书共分 9 章：第 1 章全面分析了计算机网络的基本安全问题，介绍了网络安全的基本概念、内容和方法，以及当前病毒发展的趋势和最新的反病毒技术；第 2 章重点介绍了网络攻击与防范措施；第 3 章介绍了拒绝服务与数据库安全相关知识；第 4 章重点介绍了计算机病毒与木马的概念，以及攻击防范技术；第 5 章重点介绍了入侵与攻击的基本概念，典型的攻击方法和原理，以及入侵检测方法等基本内容；第 6 章主要介绍了加密技术与虚拟专用网的相关知识；第 7 章介绍了防火墙的概念、设计原理与应用案例；第 8 章介绍了网络应用服务安全配置技术；第 9 章介绍了无线网络安全的相关知识。

本书主要由山东水利职业学院的 9 位老师编写完成。张殿明老师、杨辉老师任主编，张鹏、陈绪乾与王妍三位老师任副主编，王纬、钱玉霞、刘春燕和黄山四位老师也共同参与了本书部分章节的编写，具体工作完成情况如下。

全书由张殿明策划、组织编写、修改校对和统稿。第 1 章由张殿明编写，第 2 章由王纬编写，第 3 章由陈绪乾编写，第 4 章由王妍编写，第 5 章由钱玉霞编写，第 6 章由刘春燕编写，第 7 章由黄山编写，第 8 章由张鹏编写，第 9 章由杨辉编写。马洪波老师参与了本书部分章节文字的修改和校对工作。

本书在技术审核及内容编选上得到了徐州师范大学姜芳艽博士的大力支持，并担任本书的主审，在此感谢她所给予的建议。限于编者的水平，书中有不当甚至错误之处，诚恳广大读者提出宝贵意见。

编　者

目　录

第 1 章　网络安全概述

【本章要点】

通过本章的学习，可以了解网络安全的现状及发展趋势，掌握其定义。了解网络安全主要表现的几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理安全等。了解当前最先进的反病毒技术。

1.1　网络安全的内涵

近十年来，随着计算机和网络技术在社会生活各方面的广泛应用，计算机和计算机网络已经成为人们生活中不可或缺的重要组成部分。计算机网络具有的开放性、交互性和分散性等特点，使其很容易受到干扰和攻击。计算机网络安全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、应用数学和信息论等多种学科的综合性学科，其涉及访问控制、身份验证和加密传输等多个方面的知识。

在网络世界里，黑客攻击事件频频发生，现在全世界平均不足 20 秒就发生一次黑客入侵事件，而全球每年因网络安全问题造成的经济损失也达数千亿美元。现在，我们使用的常用存储介质(如 U 盘、CD、DVD 等)，都可能携带恶性代码；收发邮件、上网浏览、下载软件以及即时通讯都可能被黑客利用而受到攻击；一台新计算机在连接到网上不到 15 分钟即可能被扫描到。所以我们所处的网络环境已经非常不安全。

随着全球信息高速公路的建设和发展，个人、企业乃至整个社会对信息技术的依赖程度越来越大，一旦网络系统安全受到严重威胁，不仅会对个人造成不可避免的损失，严重时将会给企业、社会、乃至整个国家带来巨大的经济损失。因此，提高对网络安全重要性的认识、增强防范意识、强化防范措施，不仅是各个企业、组织要重视的问题，也是保证信息产业持续稳定发展的重要保证和前提条件。

1.1.1　网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露。系统连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于如何防范外部非法攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用都必须考虑和必须解决的一个重要问题。

1.1.2 网络安全的特征

网络安全一般应包括以下五个基本特征。

(1) 保密性：确保信息不泄露给非授权用户。

(2) 完整性：确保数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

(3) 可用性：确保可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性：确保对信息的传播及内容具有控制能力。

(5) 可审查性：确保出现安全问题时提供依据与手段。

1.2 网络安全分析

从网络运行和管理者的角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家安全的信息进行过滤和防堵，避免机要信息泄露，避免对社会造成危害、给国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网(Intranet)、企业外部网(Extranet)、全球互联网(Internet)的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断的提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理安全等。

对于网络安全问题，为了防患于未然，首先要了解网络安全的根源，然后制定相应的安全策略，做到事前主动防御、事发灵活控制和事后分析追踪。避免造成损失。

1.2.1 物理安全

网络的物理安全是整个网络系统安全的前提，也是整个组织安全策略的基本元素。总体来说，物理安全的风险主要有：地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获等。因此要尽量避免网络的物理安全风险，对于足够敏感的数据和一些关键的网络基础设施，可以在物理上和多数公司用户分开，并采用增加的身份验证技术(如智能卡登录、生物验证技术等)控制用户对其物理上的访问，从而减少安全破坏的可能性。

1.2.2　网络结构安全

网络拓扑结构设计也直接影响到网络系统的安全性。当外部与内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也可能影响在同一网络上的许多其他系统。通过网络传播，还会影响到连上 Internet/Intranet 的其他的网络；因此，我们在设计时有必要将公开服务器(WEB、DNS、EMAIL 等)和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

1.2.3　系统安全

系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。不管基于桌面的操作系统还是基于网络的操作系统，都不可避免地存在诸多的安全隐患，如非法存取、远程控制、缓冲区溢出以及系统后门等。从各个操作系统厂商不断发布的安全公告以及系统补丁可见一二。可以确切地说，没有完全安全的操作系统。不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。因此不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置。而且，必须加强登录过程的认证(特别是在到达服务器主机之前的认证)，确保用户的合法性；其次应该严格限制登录者的操作权限，将其能完成的操作限制在最小的范围内。

1.2.4　应用系统安全

应用系统的安全跟具体的应用有关，它涉及面广。应用系统的安全是动态的。应用的安全性也涉及信息的安全性，它包括很多方面。

1. 应用系统的安全是动态的、不断变化的

应用程序配置和漏洞通常是恶意软件攻击或利用的目标。如攻击者可以通过诱使用户打开受感染的电子邮件附件攻击系统或使恶意软件在整个网路上达到传播的目的。而其他如 WWW 服务、即时通讯、FTP 服务以及 DNS 服务等都存在不同程度的安全漏洞，只有通过专业的安全工具不断发现漏洞、修补漏洞，提高系统的安全性，才能有效防止恶意的攻击。

2. 应用的安全性涉及信息、数据的安全性

信息的安全性涉及机密信息泄露、未经授权的访问、假冒信息、破坏信息完整性、破坏系统的可用性等。在某些网络系统中，涉及很多机密信息，如果一些重要信息被窃取或破坏，在经济、社会和政治方面将造成严重的影响。因此，对用户使用计算机必须进行身份认证，对于重要信息的通讯必须授权，传输必须加密。采用多层次的访问控制与权限控制手段，实现对数据的安全保护；采用加密技术，保证网上传输信息包括管理员口令与账户、上传信息等的机密性与完整性。

1.2.5 管理的安全

管理是网络安全最重要的部分。责权不明，安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其他一些安全威胁时(如内部人员的违规操作等)，无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案。因此，最可行的做法是把健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是局域网建设过程中重要的一环。

1.3 网络安全的现状和发展趋势

1.3.1 概况

据国内知名信息安全厂商瑞星公司与金山安全中心统计、研究表明，病毒制造的模块化、专业化以及病毒“运营”模式的互联网化成为2008年中国计算机病毒发展的三大显著特征。目前“病毒产业互联网化”趋势已经非常明显，各种流行软件、浏览器插件、网站的漏洞层出不穷。同时，黑客的“逐利性”依旧没有改变，网页挂马、漏洞攻击已成为黑客获利的主要渠道。

2008年，两大公司用不同的标准对新增病毒进行了统计，得出相同的结论：2008年的病毒数量比2007年有很大增长(瑞星统计为增长12倍以上，金山统计为增长48倍)。其中“网页挂马”所传播的木马、后门等病毒占据90%以上，网页浏览已经成为病毒传播的最主要渠道。从病毒的运作模式看，2008年病毒多采用下载器关闭安全软件，然后下载大量盗号木马到用户电脑的方式盗取用户的网游账号和网银账号，再发送到黑客的数据库，具有极其明显的经济利益特征。

2009年央视“3·15”晚会上曝光的大量个人信息被倒卖的案例中，一个网名叫“顶狐”的黑客，也是个病毒制造高手，利用自己编写的木马程序，每天盗取的个人信息就达到3G，相当于15亿个汉字或100本辞海字典这么大的信息量。而这些信息都是以“打包”的方式出售，相当于“批发”。其经营方式是：“顶狐”首先对获得的各种个人信息进行分类整理，将其中网络游戏号、密码等信息廉价出售，而网上银行用户信息则以400元每G的价格“打包”售出。有了账号和密码，银行卡里的钱就可以随意支取了。因此，一些用户在不知不觉中，银行卡里的钱已变成了零。

黑客入侵和木马攻击越来越猛烈，网站遭受破坏的事件时有发生。网络安全已经成为当今信息社会中存在的重大现实问题，不仅影响网民的个人生活，而且与国家安全息息相关，影响国家的经济、政治和军事安全。

瑞星安全专家指出，木马病毒的编写、传播到出售的产业链已经完全互联网化，这也是导致病毒数量暴增和危害增大的根本原因，其杀伤力、传播能力、破坏性与前几年相比有大幅度的提高。整个反病毒行业已经面临全面性的变革。

1.3.2　电脑病毒疫情统计

1. 瑞星公司 2008 年电脑病毒疫情统计

2008 年 1 月至 10 月，瑞星公司共截获新病毒样本 9306985 个，是去年同期的 12.16 倍。其中木马病毒 5903695 个，后门病毒 1863722 个，两者之和超过 776 万，占总体病毒的 83.4%。如图 1-1 和图 1-2 所示。

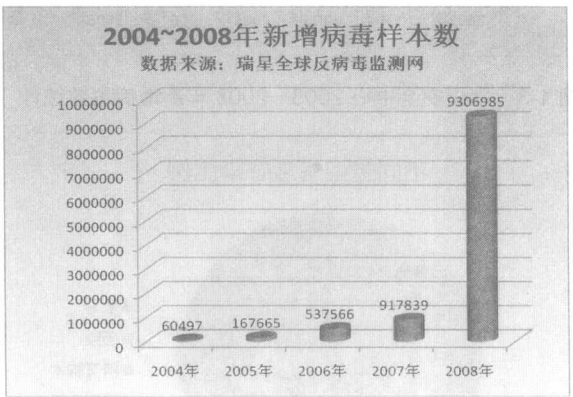


图 1-1　瑞星公司 2004—2008 年新增病毒样本数统计

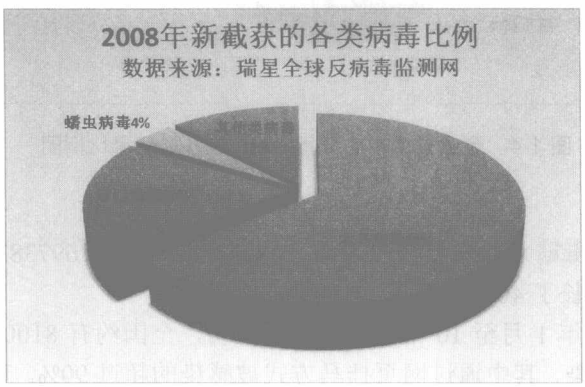


图 1-2　瑞星公司分析 2008 年各类病毒比例图

2. 金山安全中心 2008 年电脑病毒疫情统计

据金山毒霸“云安全”中心监测数据显示：2008 年，金山毒霸共截获新增病毒、木马 13899717 个，与 2007 年相比增长 48 倍。在新增的病毒、木马中，新增木马数为 7801911 个，占全年新增病毒、木马总数的 56.13%；黑客后门类占全年新增病毒、木马总数的 21.97%；而网页脚本所占比例从去年的 0.8%跃升至 5.96%，成为增长速度最快的一类病毒。如图 1-3 和图 1-4 所示。

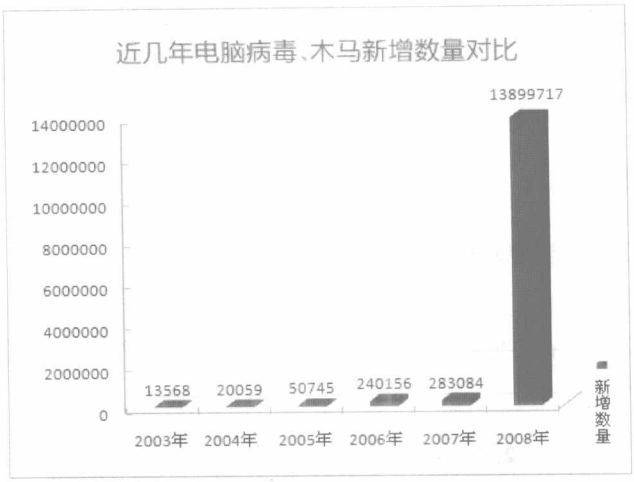


图 1-3　金山安全中心 2003—2008 年新增病毒数统计

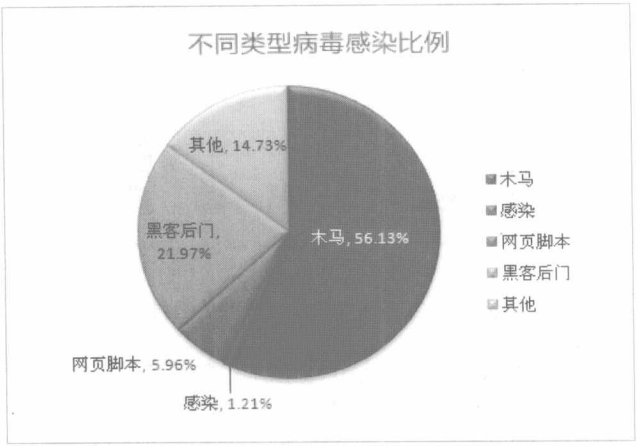


图 1-4　金山安全中心分析 2008 年各类病毒比例图

3. 疫情介绍

2008 年，据金山毒霸“云安全”中心统计数据，全国共有 69738785 台计算机感染病毒，与 2007 年相比增长了 40%。

瑞星公司对 2008 年 1 月至 10 月的数据统计表明，全国约有 8100 多万台电脑(包含企业用户)曾经被病毒感染，其中通过网页挂马方式被感染的超过 90%。瑞星于 2008 年 10 月份，对 1 万台上网电脑的抽样调查，发现这些电脑每天遇到的挂马网站，高峰期达到 8428 个，最低也有 1689 个，考虑单台电脑访问多个挂马网站的可能，平均每天也有 30%的网民访问过挂马网站，中国内地已经成为全球盗号木马最猖獗的地区之一。

360 安全专家石晓虹博士公开表示：整个地下木马产业从业人员已接近百万的规模，仅 2008 年一年就制造了各种旨在盗号、盗隐私、抓“肉鸡”的木马为 9743122 种!

目前流行的各种热门网站、客户端软件和浏览器，都存在着众多漏洞和安全薄弱点，使得用户遭受攻击的几率大大增加。而且，随着黑客—病毒产业链臻于完善，支撑互联网

发展的多种商业模式都遭到了盗号木马、木马点击器的侵袭，使得用户对于网络购物、网络支付、网游产业的安全信心遭到重创，必会影响整个互联网的健康、有序的发展。

1.3.3　计算机病毒、木马的特点分析

1. 病毒制造趋于“机械化”

“病毒制造机”是网上流行的一种制造病毒的工具，一个人不需要任何专业技术就可以手工制造生成病毒。黑客便可根据自己对病毒的需求，很简单地在相应的制作工具中定制病毒功能。病毒傻瓜式的制作导致病毒进入“机械化”时代。

病毒的机械化生产导致病毒数量的爆炸式增长。反病毒厂商传统的人工收集以及鉴定方法已经无法应对迅猛增长的病毒。

2. 病毒制造具有明显的模块化、专业化特征

黑客组织按功能模块发外包生产或采购技术先进的病毒功能模块，使得病毒的各方面功能都越来越“专业”，病毒技术得以持续提高和发展，对网民的危害越来越大，而解决问题也越来越难。例如 2008 年年底出现的“超级 AV 终结者”集病毒技术之大成，是模块化生产的典型代表。

在专业化方面，目前的病毒产业链条由四个部分组成：挖掘安全漏洞、制造网页木马、制造盗号木马、制造木马下载器(病毒下载者)。这些环节形成了分工明确、效率快捷的工业化“生产线”，每个环节各司其职，专业化趋势明显。

3. 病毒产业互联网化

黑客组织运营模式已经完全互联网化，攻击的方式一般为：网站入侵→植入木马→网民访问挂马网站→受到漏洞攻击而“不知不觉”中毒。这种传播方式的特点是快速、隐蔽性强、适合商业化运营。

由于病毒制造、传播、牟利的流程完全互联网化，比传统的黑客行为更容易带来经济利益。目前已经形成了一个巨大无比的黑色产业，黑客可以选择自己擅长的环节运作，从而使得产业的运作效率更高。

从统计数据来看，活跃病毒中 90%以上都与经济利益直接挂钩。从网页挂马占到病毒传播总量 90%以上这个明显的特征我们可以看出，互联网最为基础、最为普遍的应用——网页浏览是黑客利用的最为深入透彻的传播渠道。如图 1-5 所示，我们可以简单了解病毒产业是如何互联网化的。

1)　漏洞的挖掘和交易

软件存在安全漏洞是当前病毒传播的一个重要前提，通过用户电脑系统中安装的软件存在的漏洞，病毒可以快速地在用户不知情的情况下进入用户电脑。现在，软件漏洞挖掘已经成为病毒产业链里的一环。

黑客专门从系统上寻找漏洞，之后到地下交易网站进行出售，从而获得不菲的黑色收入。

黑客组织购买了漏洞信息后，利用这些信息编写强大的新病毒，在软件厂商还毫无觉察时，新病毒已经在互联网上大量传播，因此不能及时提供修复补丁，造成 0day 攻击蔓延。

2) 网页挂马的策略

目前，病毒一般不能进行主动传播，绝大多数木马、后门都是通过网页挂马进行的，它是一种“被动”的病毒传播方式，用户只有去访问挂马网站，才会遭到木马病毒的侵袭。

为了让更多的用户主动访问挂马网站，黑客采用多种方式来提高挂马网站的流量，以某中文网被“挂马”为例，它的页面访问量每天接近 100 万，在 2009 年 3 月 11～12 日间，因未打补丁而导致“中马”的用户很快突破了 12 万，其中如果有一半用户玩网游，他们都将面临账号失窃的风险，保守估计，黑客组织也可盗取 3 万以上的游戏账户，一个游戏账户可以卖到 50 元以上，而攻下这类安全性较低的网站花销不过数千元，一次成功的入侵带来的利润可想而知，而如果向色情网站或个人网站购买 100 万流量，也仅仅需要 1 万元左右。有的黑客组织，会雇佣专门的人去入侵正常网站，如门户网站、新闻网站、热门论坛等，在其中植入木马，或者对自己的挂马网站进行 SEO 优化。当用户搜索“美女”、“电影”等热门关键词的时候，这些带毒网站会排在搜索结果的前几页，从而带来大量的用户。还有利用新兴的 SNS 网站散发挂马链接，通过站内信、博客回帖等形式，吸引网民访问。现在热门的 Web 2.0 网站，几乎都遭到过此类带毒链接的侵扰。

3) 网页挂马常用的漏洞

目前，黑客仍然利用漏洞传播木马，主要手段是网页挂马，但 RealPlayer、迅雷、PPlive 等流行软件出现的严重漏洞，也被黑客利用传播木马。2008 年 4 月份爆出的 Adobe Flash Player 漏洞成为当年最为流行的漏洞，有 18%的木马通过该漏洞侵入用户电脑。

只有不良网站才会带毒、才会被挂马，坚持良好的浏览习惯，就可以躲避盗号木马等病毒的侵袭，这样的观念已经过时，那些所谓的“正常网站、大中型网站，还有明星粉丝的聚集地”正在整个木马链条中发挥着越来越重要的作用。

根据瑞星统计，2008 年黑客常用的各种漏洞共有 16 个(统计情况如表 1-1 所示)，正是因为这些漏洞的存在，而且用户又没有安装漏洞补丁，就使得木马病毒很容易地侵入用户电脑。

表 1-1 常用软件被利用统计表

漏洞名称	在被利用漏洞中所占比例
Adobe Flash Player	18%
RealPlayer 10/11	10%
Microsoft Date Access Components (ms06-014)	8%
Windows ant (ms07-017)	8%
迅雷看看 ActiveX	7%
暴风影音 II ActiveX	7%
PPlive ActiveX	7%
PPS ActiveX	7%
Microsoft Office 2003 (ms08-011)	5%
Microsoft Office (ms08-056)	5%
Windows Media Player (ms08-053)	3%