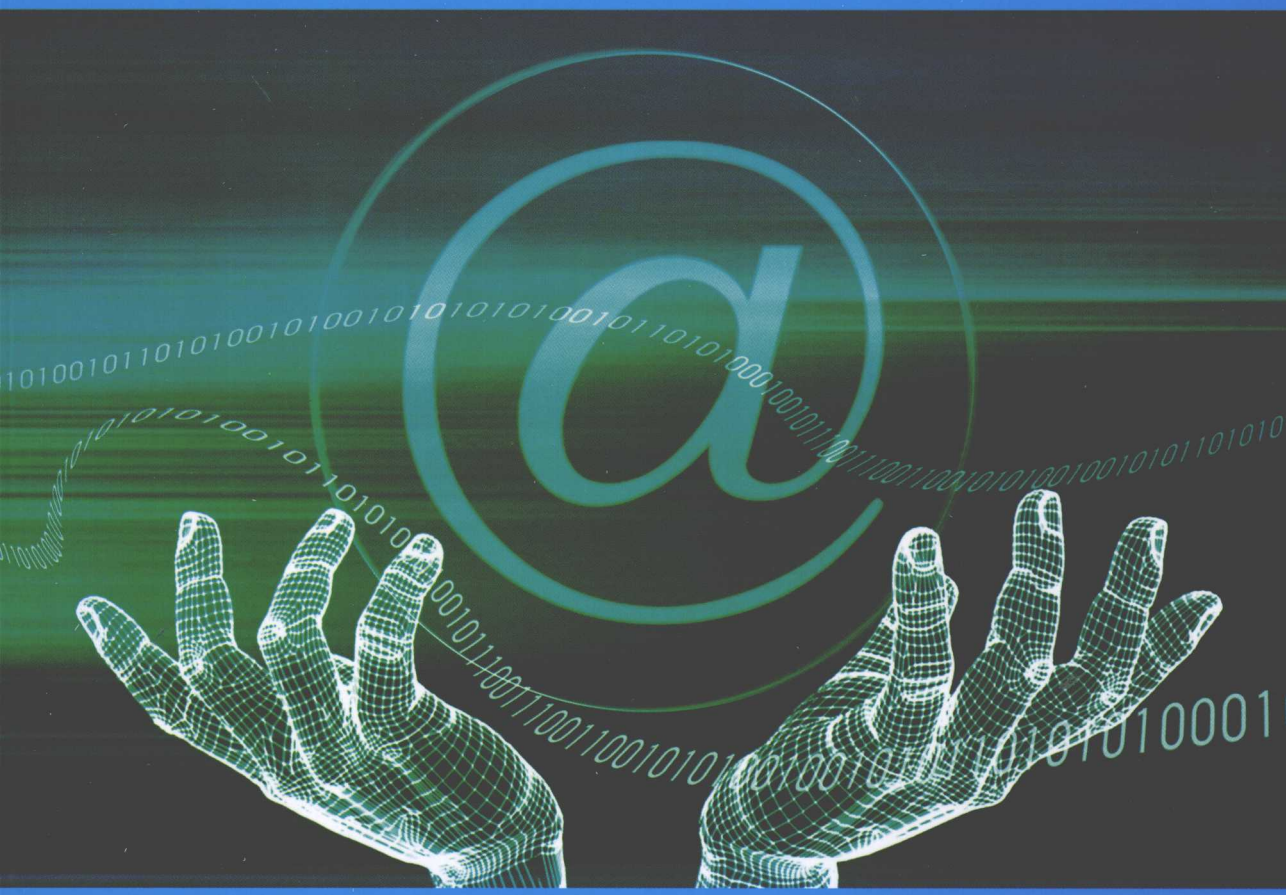
高职高专
网络专业系列规划教材

新世纪

计算机网络安全技术

新世纪高职高专教材编审委员会组编
主编 薛庆水 朱元忠 主审 唐礼勇



大连理工大学出版社

新世纪

高职高专网络专业系列规划教材

计算机网络安全技术

主　审　唐礼勇

主　编　薛庆水　朱元忠　副主编　汪　进　所　辉　王巧巧　梁立哲

JISUANJI WANGLUO ANQUAN JISHU

大连理工大学出版社

DALIAN UNIVERSITY OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

计算机网络安全技术 / 薛庆水，朱元忠主编. —大连：大连理工大学出版社，2008.2
高职高专网络专业系列规划教材
ISBN 978-7-5611-3856-4

Ⅰ.计… Ⅱ.①薛… ②朱… 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(2008)第 018527 号

大连理工大学出版社出版
地址：大连市软件园路 80 号 邮政编码：116023
电话：0411-84708842 邮购：0411-84703636 传真：0411-84701466
E-mail：dutp@dutp.cn URL：http://www.dutp.cn
大连天正华延彩色印刷有限公司印刷 大连理工大学出版社发行

幅面尺寸：185mm×260mm 印张：17.25 字数：397 千字
印数：1～4000
2008 年 2 月第 1 版 2008 年 2 月第 1 次印刷

责任编辑：付 亮 责任校对：张爱华
封面设计：苏儒光

ISBN 978-7-5611-3856-4 定 价：26.00 元

总 序

我们已经进入了一个新的充满机遇与挑战的时代，我们已经跨入了21世纪的门槛。

20世纪与21世纪之交的中国，高等教育体制正经历着一场缓慢而深刻的革命，我们正在对传统的普通高等教育的培养目标与社会发展的现实需要不相适应的现状作历史性的反思与变革的尝试。

20世纪最后的几年里，高等职业教育的迅速崛起，是影响高等教育体制变革的一件大事。在短短的几年时间里，普通中专教育、普通高专教育全面转轨，以高等职业教育为主导的各种形式的培养应用型人才的教育发展到与普通高等教育等量齐观的地步，其来势之迅猛，发人深思。

无论是正在缓慢变革着的普通高等教育，还是迅速推进着的培养应用型人才的高职教育，都向我们提出了一个同样的严肃问题：中国的高等教育为谁服务，是为教育发展自身，还是为包括教育在内的大千社会？答案肯定而且惟一，那就是教育也置身其中的现实社会。

由此又引发出高等教育的目的问题。既然教育必须服务于社会，它就必须按照不同领域的社会需要来完成自己的教育过程。换言之，教育资源必须按照社会划分的各个专业（行业）领域（岗位群）的需要实施配置，这就是我们长期以来明乎其理而疏于力行的学以致用问题，这就是我们长期以来未能给予足够关注的教育目的问题。

如所周知，整个社会由其发展所需要的不同部门构成，包括公共管理部门如国家机构、基础建设部门如教育研究机构和各种实业部门如工业部门、商业部门，等等。每一个部门又可作更为具体的划分，直至同它所需要的各种专门人才相对应。教育如果不能按照实际需要完成各种专门人才培养的目标，就不能很好地完成社会分工所赋予它的使命，而教育作为社会分工的一种独立存在就应受到质疑（在市场经济条件下尤其如此）。可以断言，按照社会的各种不同需要培养各种直接有用人才，是教育体制变革的终极目的。

随着教育体制变革的进一步深入，高等院校的设置是否会同社会对人才类型的不同需要一一对应，我们姑且不论。

但高等教育走应用型人才培养的道路和走研究型(也是一种特殊应用)人才培养的道路,学生们根据自己的偏好各取所需,始终是一个理性运行的社会状态下高等教育正常发展的途径。

高等职业教育的崛起,既是高等教育体制变革的结果,也是高等教育体制变革的一个阶段性表征。它的进一步发展,必将极大地推进中国教育体制变革的进程。作为一种应用型人才培养的教育,它从专科层次起步,进而应用本科教育、应用硕士教育、应用博士教育……当应用型人才培养的渠道贯通之时,也许就是我们迎接中国教育体制变革的成功之日。从这一意义上说,高等职业教育的崛起,正是在为必然会取得最后成功的教育体制变革奠基。

高等职业教育还刚刚开始自己发展道路的探索过程,它要全面达到应用型人才培养的正常理性发展状态,直至可以和现存的(同时也正处在变革分化过程中的)研究型人才培养的教育并驾齐驱,还需假以时日;还需要政府教育主管部门的大力推进,需要人才需求市场的进一步完善发育,尤其需要高职高专教学单位及其直接相关部门肯于做长期的坚忍不拔的努力。新世纪高职高专教材编审委员会就是由全国100余所高职高专院校和出版单位组成的旨在以推动高职高专教材建设来推进高等职业教育这一变革过程的联盟共同体。

在宏观层面上,这个联盟始终会以推动高职高专教材的特色建设为己任,始终会从高职高专教学单位实际教学需要出发,以其对高职教育发展的前瞻性的总体把握,以其纵览全国高职高专教材市场需求的广阔视野,以其创新的理念与创新的运作模式,通过不断深化的教材建设过程,总结高职高专教学成果,探索高职高专教材建设规律。

在微观层面上,我们将充分依托众多高职高专院校联盟的互补优势和丰裕的人才资源优势,从每一个专业领域、每一种教材入手,突破传统的片面追求理论体系严整性的意识限制,努力凸现高职教育职业能力培养的本质特征,在不断构建特色教材建设体系的过程中,逐步形成自己的品牌优势。

新世纪高职高专教材编审委员会在推进高职高专教材建设事业的过程中,始终得到了各级教育主管部门以及各相关院校相关部门的热忱支持和积极参与,对此我们谨致深深谢意;也希望一切关注、参与高职教育发展的同道朋友,在共同推动高职教育发展、进而推动高等教育体制变革的进程中,和我们携手并肩,共同担负起这一具有开拓性挑战意义的历史重任。

新世纪高职高专教材编审委员会

2001年8月18日

前言

随着信息技术的迅猛发展和广泛应用，社会信息化进程不断加快，信息网络的基础性、全局性作用日益增强。社会对信息化的依赖性也越来越强，信息网络的安全问题愈加重要。

当前，伴随着我国社会主义市场经济的快速发展，中国即将或已经成为世界制造业中心，各行各业越来越需要具有综合职业能力和全面素质的，直接工作在生产、技术、管理和服务第一线的应用型、技能型的高级实用人才。可以预见，高等职业技术教育即将和高等教育的本科教育相提并论，并且在我国高等教育体系中占有相当重要的地位。

高职教育作为我国高等教育的一个重要组成部分，其培养目标是具有必要理论知识和较强实践能力的高等技术应用型专门人才。它的人才培养以适应生产、建设、管理、服务第一线需要的高等技术应用型专门人才为根本任务；以适应社会需要为目标；以培养技术应用能力为主线；以突出职业性、实践性、适应性和地方性为特点。在计算机教学中，应以传授应用知识为主，强调操作使用，注重培养学生利用计算机开展专业技术分析、解决各种技术问题的意识，培养学生的自学能力和创造性学习的能力为目标。

密切结合高职教育的特点，在编写本教材时，对于计算机网络安全的理论知识和工作原理介绍得简单一些，更多的内容侧重于对计算机具体网络安全技术的应用的介绍，体现出注重培养学生实际应用技术能力的特点。在内容的安排上，每章后面都安排了适量的练习与实验题目，并且都配有参考答案，方便教师的教学与学生的自学。在编写的过程中，力求体现教材的系统性、先进性和实用性。

全书共分14章，第1章介绍了有关计算机网络安全的各种基本概念、基本知识，使学生对计算机网络安全有一个基本的、总体的认识和了解。第2章介绍了网络安全的基本概念和网络安全的体系框架等，要求了解相关的概念，掌握网络安

全的体系框架和网络安全系统的功能，了解 OSI 参考模型的安全问题。第 3 章介绍了网络数据包的结构与数据包截获的原理和分析方法，讲述了 Sniffer 软件的使用方法，使学生对网络数据包的结构与截获和分析有一个全面的认识。第 4 章介绍了数据加密技术，在阐述了一些基本概念之后给出了几种在 Internet 中常见的数据加密技术，使学生掌握数据保护的有关知识。第 5 章介绍密钥管理方法，包括密钥的管理内容、分配技术，重点介绍与当前网络应用的发展密切相关的公开密钥管理体制，使学生能掌握密钥的管理方法和管理体制。第 6 章介绍数据完整性保护技术，包括信息摘要技术和数字签名技术，使学生能掌握保护数据完整性的各种技术。第 7 章介绍数据鉴别技术的基本方法以及在 Internet 中常见的数据鉴别技术，使学生能够理解和掌握各种数据鉴别技术。第 8 章介绍单机和网络的访问控制问题，使学生了解访问控制的基本原理和常用的防火墙技术。第 9 章介绍了计算机病毒的概念、计算机病毒的发展史与危害，以及计算机病毒的主要特性、计算机病毒的分类、查杀与防范方法等。第 10 章以 Internet 的安全为背景，介绍了网络攻防技术的基本原理，使学生能够了解各种网络入侵和网络攻击技术，掌握安全防范和安全监测的基本原则和一般方法。第 11 章以 IETF 安全领域中一些工作组的工作内容为背景介绍了 Internet 基础设施安全方面的一些新进展，使学生能够追踪有关网络安全领域前沿的研究方向和研究课题。第 12 章介绍 Internet 部分网络基础设施 DNS 及 PGP。第 13 章介绍了操作系统安全的基本概念、访问控制的概念、类型与措施、Windows 系列操作系统、UNIX 和 Linux 系统的安全漏洞与安全措施。第 14 章介绍了计算机信息系统安全评价标准，要求掌握美国可信计算机系统评价标准中对计算机系统的安全划分的七个级别，三个大类。

本书内容安排合理，逻辑性强，文字简明，循序渐进，通俗易懂，适合高职高专信息安全专业学生的专业教学使用，也适合计算机类本科专业学生和各种网络安全的培训班使用。

本书由薛庆水、朱元忠任主编。朱元忠编写了第 1～2、11、12、14 章，汪进编写了第 3、9 章，梁立哲编写了第 4 章，薛庆水编写了第 5～7、13 章，在统稿的过程中，朱元忠对第 8～12 章进行了审阅，全书由薛庆水统阅定稿。在书的编写过程中，还有其他一些作者参与。

在本书的立项、大纲的编写和内容的确定以及编写过程中得到了大连理工大学出版社各位同志的大力支持和帮助，在此表示衷心的感谢。特别感谢北京大学计算机科学技术系的唐礼勇副教授在大纲的修改与确定中所提出的宝贵意见和建议。同时，感谢刘远生教授在教材编写过程中给予的指导和帮助。

由于时间仓促和作者水平有限，书中难免存在错误、缺点与不足，恳请各位学者、专家、老师和同学提出宝贵意见。

所有意见和建议请发往：gzjckfb@163.com

联系电话：0411-84707492

编　者

2008 年 1 月

目　录

第1章 网络安全概述

本章重点与难点

网络安全基本概念。

教学要求

介绍网络安全的定义，通过讲述历史上的网络安全事件，激发学生学习网络安全的兴趣，结合网络安全事件的介绍，讲述网络安全的基本概念。

1.1 网络安全的定义

计算机网络安全是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害，即指计算机、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到破坏、更改和泄露，确保系统能连续可靠正常地运行，使网络服务不中断。计算机网络安全从其本质上来讲就是系统上的信息安全。计算机网络安全是一门涉及计算机科学、网络技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性科学。

从广义来说，凡是涉及到计算机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计算机网络安全的研究领域。所以，广义的计算机网络安全还包括信息设备的物理安全性，诸如场地环境保护、防火措施、防水措施、静电防护、电源保护、空调设备、计算机辐射和计算机病毒等。

网络安全的定义中，涉及一些网络领域的专业术语，我们可以从后面的学习中逐渐深入了解它们。

1.2 网络安全事件速览

1.2.1 网络安全事件的起源

1979年，年仅15岁的凯文·米特尼克仅凭一台电脑和一部调制解调器闯入了北美空中防务指挥部的计算机主机。在“以信任对方”为前提的高校实验室中诞生的诸多网络协议，不仅让当时的恶意攻击者有机可乘，而且时至今日也成为一些攻击的原罪，如利用TCP/IP三次握手的SYN FLOOD、SMTP的伪造信息头和更改源地址的重定向攻击等等，都是利用了协议的漏洞。

1983年，美国联邦调查局首次逮捕了6名少年黑客，这6名少年黑客被控侵入60多台电脑，其中包括斯洛恩·凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室。用计算机从事破坏活动的性质被确定为“犯罪”，就是从这时候开始的。

1987年，美国联邦执法部门指控16岁的赫尔伯特·齐恩闯入美国电话电报公司的内部网络和中心交换系统。齐恩是美国1986年“计算机欺诈与滥用法案”生效后被判有罪的第一人。利用计算机和网络进行犯罪的“有法可依”，给假借黑客之名进行犯罪之实的家伙们敲响了警钟。

1988年，美国康奈尔大学研究生罗伯特·莫里斯向互联网传输了一个蠕虫程序，感染了6000多个系统——几乎占当时互联网的十分之一。同年，在发现有黑客入侵军事网的一部联网电脑后，美国国防部切断了非保密军事网与阿帕网（早期互联网）之间的物理连接。有人问过，“怎样才能做到服务器绝对安全?”回答是：“拔掉网线!”但这样就不能提供服务了。因此，所有尽责的网络管理员所能做到的，只是尽力接近安全而已。

1.2.2 网络——盗窃钱财的新途径

早期的网络安全事件，多因黑客为炫耀技术而起，这也是时至今日，黑客们制造的许多网络安全事件仍能得到大多数网民原谅的主要原因。但是随着互联网应用的深入发展，网络蕴藏着巨大的商机和通过网络产生的巨大的经济利益驱使许多技术高超的黑客走向商业犯罪。

1. 世界范围内的网络盗窃

1995年，“世界头号电脑黑客”凯文·米特尼克被捕。他被指控闯入许多电脑网络，包括入侵北美空中防务体系和美国国防部，偷窃了2万个信用卡号和复制软件。同年，俄罗斯黑客列文在英国被捕。他被指控用笔记本电脑从纽约花旗银行非法转移至少370万美元到世界各地由他和他的同党控制的账户。这类事件不断上演，是不是将你心目中的黑客拉下了神台?

2. “网络钓鱼”钓你钱财

2005年1月，一个假冒中国工商银行的网站出现在互联网上，诱骗银行卡持有者的账户和密码，并导致多人的银行存款被盗，直接经济损失达800000元人民币。事发后，引起各大银行的重视，中行、工行和农行等多家银行均迅速在其网站上发表“敬告客户”或“安全提

示”的信息，提示其网上银行客户登录合法网址。“网络钓鱼”作为一种网络诈骗的新手段，出现在国人面前。

在中国，“网络钓鱼”暂时还没有造成过多的损失，但随着宽带网络进一步普及，用户将面临更多的线上交易安全风险。2004 年，国家计算机网络应急技术处理协调中心共接到网络仿冒报告 223 起，仿冒对象主要是金融网站和电子商务网站。而在 2002 年和 2003 年，每年只有一起，同比增长了上百倍。2005 年，假冒网站数量进一步增加。

“网络钓鱼”这种攻击方式利用欺骗性的电子邮件、手机短信以及伪造的 Web 站点等来进行诈骗活动，欺骗者通常会找一个看似正当的理由。例如：提示你为了保证你的银行卡安全，要求你在线更改你的信用卡密码，然后将用户引诱至某个著名企业的假冒网站。这些假冒的网站域名与企业真正的域名非常相近，如假冒中国工商银行域名是 www. 1cbc. com. cn，与中国工商银行网站 www. icbc. com. cn，也只是“1”和“i”一字之差。

在假冒网站的首页通常会有一个仿冒的密码输入框，提示你输入账户和密码，然后将用户输入的内容通过邮件等方式发给欺骗者。受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名和口令等内容。“网络钓鱼”这种攻击方式最大的特点是不需要主动攻击，欺骗者只需要静静等候上当的“鱼儿”就可以了。

网上交易已经是大家相当熟悉的交易方式了，网上交易的安全性是整个网上交易的重心。可是频频发生的假冒网上银行和银行卡短信欺诈事件让人们在感受到互联网带来的便捷的同时，也感受到它极大的风险性。好在现在国家立法对网上交易进行规范，相信随着法规的不断完善和人们安全意识的提高，“网上钓鱼”这种欺骗手段终将消失。

3. 网上团伙作案逐渐呈现

日前，宁波警方在安徽警方的配合下，将正在网吧里聊天的徐某抓获。这位年仅 17 岁的少年就是年初发生的利用“黑客”技术盗窃网上银行存款一案的主谋。而在他的 QQ 好友名单里竟有近二百名“志同道合”的少年“黑客”。

2005 年 1 月 4 日，宁波张女士的网易电子邮箱收到一封自称是网易公司员工发来的邮件，说张女士的邮箱中奖了，只需提供本人身份证号码和家庭住址即可得到一台价值近万元的索尼 DV 摄录机。信里还留有联系电话和电子邮箱。第二天，张女士把身份证号码和家庭住址告诉了对方。当晚，她发现网上银行账户里的存款少了近五千元人民币。1 月 6 日，张女士赶紧把十多万余款全部取出并向宁波江北区警方报案。

经过调查，警方发现电子邮件来自注册在成都的一个私人网站，登记邮编是安徽省马鞍山市新市镇，在案发后两天就关闭了。与此同时，警方综合另外几条线索，初步断定嫌疑人很可能是新市镇当地人。历时两个月的不懈追踪，嫌疑人徐某终于被抓获。

徐某交代，因为现在互联网上的很多游戏都需要用钱去购买虚拟币才能玩，所以他学了些“黑客”知识后开始盗用他人的虚拟币，再转卖给他人，每月收入可达数千元。因为一条偶然看到的新闻，他就开始了通过骗取他人网上账户信息盗取存款的不法行为。如此简便的挣钱方式一度让他特有成就感。也因此，这位来自普通家庭的少年一直混迹在安徽、湖南、湖北等地网吧，花钱如流水，身边女友不断。

然而，相对于案件个体，意外在徐某 QQ 上发现的近二百位“少年黑客兵团”名单更让警方震惊和担忧。这些同龄人唯徐某马首是瞻，按各自的“攻关”级别以“总、军、师”和“首长”等头衔称呼，俨然就是一个组织严密的“少年黑客兵团”。徐某亦承认，平时这些成员就是利

用“黑客”技术，盗窃他人的Q币和虚拟装备。

有关人士指出，互联网的兴盛引起了全球新一轮的技术更迭，但同时对社会其他领域也形成了比较大的影响。对青少年而言，他们对新事物新变化的接受力非常强，适应能力也相当高，这也就使青少年的教育问题更加复杂、严峻，必须引起足够的重视。

1.2.3 网络——宣泄情绪的途径

尽管黑客文化正在逐渐由大众回归小众，但伴随着中国外交摩擦而发生的小规模黑客冲突从来没有停止过。当我们回过头来反思黑客江湖的浮躁，我们无法忘记1999年那个愤怒的夏天，当看到白宫网站上飘扬的五星红旗时，心里忍不住浮动的快意。从根本意义上说，网络黑客所采取的手段和大学生对美国大使馆扔石头和墨水瓶没有什么两样，那只是一种宣泄的手段，追求的不是攻击性。

中国科学院新闻与传播研究所教授闵大洪说，在1998年以前，中国发生的历次大事件中，国外所能听到的只有中国官方的声音，而在印尼排华潮后，中国网民用自己的行动，将自己的声音直接传达到他们想传达的对象面前。

关于中美黑客大战以及中国网民对于印尼排华事件的反应大家可以通过互联网络查询，来了解事件的详情。

1.3 中国网络安全形势严峻

由于计算机和国际互联网的飞速普及，中国目前已经成为炙手可热的黑客攻击目标。据2005年的统计，全球每天有15万台PC机处于随时可能被攻击的失控状态，而其中有20%的PC机来自中国。

1. 盗版软件无法升级成软肋

这些可以被黑客远程攻击的PC机被称为“zombies(僵系统)”。“僵系统”的特点是，它为黑客开了一道“后门”，黑客可以随时通过远程方式对该系统“指手画脚”。一般情况下，黑客会利用这些大量的“僵系统”传播病毒或垃圾邮件。

在中国，网民越来越多，许多网民并不精通计算机技术，有些甚至还是首次接触互联网，专家指出：“对于一些没有计算机安全知识的用户，如果他们经常在线，那将是一件很危险的事情。”另外，由于很多人没有及时安装补丁程序，使得这些系统更易受到病毒的攻击。而且，关于及时更新补丁程序问题，这一直是中国计算机用户的一个“痛处”。因为中国的盗版软件比较普遍，而微软已表示，不再支持盗版Windows升级。此外，语言障碍也是导致中国计算机用户容易受到攻击的原因之一。目前，中国有20种方言，如果微软发布一款补丁程序，不可能得到所用网民的一致关注。

2. 网民应该采取预防措施

目前，计算机和互联网在中国已十分普及。据统计数据显示，每年至少有1490万台PC机出货到中国。到2010年，中国还将新增1.78亿台PC机。互联网的使用率则增长了18%。截止2007年6月，中国有网民1.62万。

用户接入互联网的方式将直接影响到病毒的传播力度。通常，黑客主要攻击的是宽带

接入用户。而目前，中国网民的宽带接入率极高，上网地点主要集中在企业、政府机构和网吧。

安全专家 RaffaelMarty 表示，要维护计算机系统安全，用户必须要采取一些基本预防措施。他说："不要从不明来源下载未知程序，通过防火墙来阻挡未知应用，并及时对系统和防病毒软件进行升级。"

SonicWall 公司安全服务副总裁 BorisYanovsky 表示，将有大量的黑客攻击事件发生，因为他们的攻击行为已经转变为出于经济目的。

1.4 网络安全概述小结

通过前面的网络安全事件，我们可以了解到目前网络安全面临的问题是比较多的，学习网络安全，就要密切关注网络安全事件发生的起因和形式，进而找出相应的防范措施，尽力使网络变得更安全。

习 题

1.1 通过网络检索，结合书中的案例，举例说明有哪几种形式的网络安全事件。

1.2 结合自己使用电脑上网的经历，介绍自己上网遇到的网络安全事件并说明解决的过程。