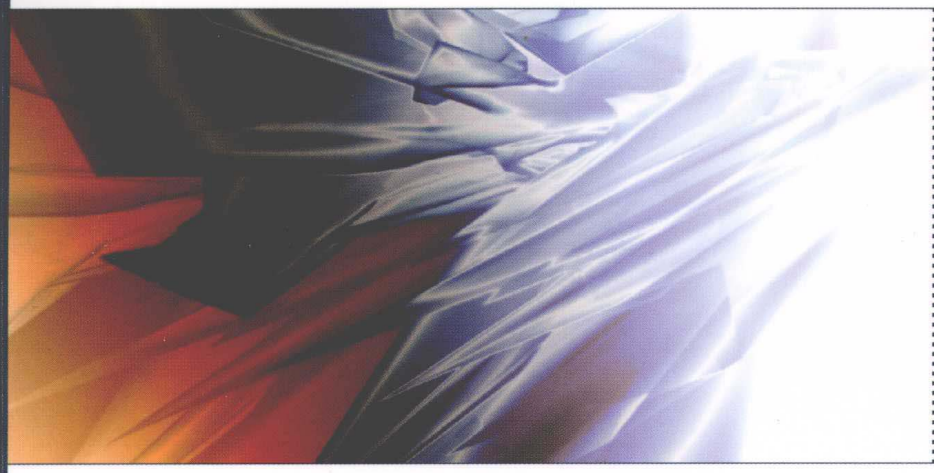
21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering



网络安全实用技术

Network Security Practical Technology

张仕斌 曾派兴 黄南铨 编著

- 结构严谨，系统性强，突出实用
- 全面阐述最新网络安全实用技术
- 满足高校培养应用型人才的需要

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering

网络安全实用技术

张仕斌 曾派兴 黄南铨 编著

人 民 邮 电 出 版 社

北 京

图书在版编目（CIP）数据

网络安全实用技术 / 张仕斌，曾派兴，黄南铨编著
-- 北京 : 人民邮电出版社，2010.12
21世纪高等院校网络工程规划教材
ISBN 978-7-115-24115-3

Ⅰ. ①网… Ⅱ. ①张… ②曾… ③黄… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第258988号

内 容 提 要

本书以网络安全实用技术为基础，全面介绍了网络安全应用技能。全书共分 9 章，重点介绍了网络安全基础知识、病毒及恶意软件清除与防御技术、计算机日常安全配置及防范技术、系统漏洞修复与扫描技术、企业服务器安全配置技术、系统灾难恢复技术、虚拟网络应用技术、文件加密和数字签名技术、PKI 技术等内容。

本书具有科学严谨的体系结构，系统性强，内容全面，突出实用。本书可作为普通高等院校计算机、通信、网络工程、信息安全等相关专业的教材，也可供计算机、通信、信息等领域研究人员和专业技术人员学习参考。

21 世纪高等院校网络工程规划教材

网络安全实用技术

◆ 编　　著　张仕斌　曾派兴　黄南铨
责任编辑　蒋　亮

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京昌平百善印刷厂印刷

◆ 开本：787×1092　1/16
印张：17.5　　2010 年 12 月第 1 版
字数：438 字　　2010 年 12 月北京第 1 次印刷

ISBN 978-7-115-24115-3

定价：32.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着网络技术的飞速发展，网络已经成为人类社会的一项关键基础设施，其应用已经深入到国家政治、经济、文化、国防建设等领域，对科学、技术、政治、经济、军事乃至人类的生活都产生了巨大的影响，数字化经济和全球电子交易一体化正在逐步形成。但是网络作为一把双刃剑，在给人们的学习、生活和工作带来便利的同时，也给保障信息安全带来了极大的挑战。网络安全不仅关系到国计民生，还与国家安全密切相关；不仅涉及到国家的政治、军事、经济等各方面，而且还影响着国家的安全和主权。而在目前网络应用的领域中，最容易被忽略的网络安全问题正在危及网络技术的进一步发展和应用，已成为世界各国关注的焦点和研究的热点。

安全性灾难事故的频繁发生，让人们对于建立在网络基础上的现代信息化生活也有了新的认识，网络安全的内涵也在不断延伸，从最初的信息保密性发展到信息的完整性、可用性、可靠性、可控性、可审查性和不可否认性，再发展到包括攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）等方面的网络安全基础理论和应用技术。作为一门综合性的交叉学科领域，网络安全技术涉及计算机科学、计算机网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论、控制论、社会学等多个学科。因此，网络安全的研究十分广泛，它涉及密码理论、安全体系结构、安全协议、网络信息分析、网络安全监控、应急处理等方面。

为满足高校培养应用型人才的需要，我们组织多年从事计算机网络与安全领域的教学、科研、学科管理等工作的骨干老师编写了本书。本书是在人民邮电出版社出版的《网络安全基础》教材的基础上，经过广泛调研和充分论证，结合当前应用最为广泛的网络安全技术，并通过研究实践编写而成的。在写作中，作者始终遵循这样一个原则：为网络安全应用领域提供一本既可以作为教学用书，也可以供专业技术人员使用的参考书。

严谨的体系结构，系统性强，突出实用，并利用通俗的语言全面阐述了最新的网络安全实用技术。全书共分 9 章，重点介绍了网络安全基础知识、病毒及恶意软件的清除与防御技术、计算机日常安全配置及防范技术、系统漏洞修复与扫描技术、企业服务器安全配置技术、系统灾难恢复技术、虚拟网络应用技术、文件加密和数字签名技术、PKI 技术等内容。

本书由张仕斌组织编写及统稿，其中第 1 章、第 4 章和第 6 章由张仕斌编写，第 2 章由陈念伟编写，第 3 章由牛婧、陈念伟编写，第 5 章由饶斌编写，第 7 章由黄南铨编写，第 8 章、第 9 章由曾派兴编写。

为了便于多媒体教学，本书配有电子教案，订购本教材的教师可到人民邮电出版社教学服务与资源网（http://www.ptpedu.com.cn）上下载。

由于作者水平有限、时间仓促，书中难免有不足和错误之处，欢迎广大读者批评指正。

编　者

2010 年 12 月于成都

目　录

第 1 章　网络安全概述

随着网络应用的快速发展，人们正突破时空的约束，享受高速网络所带来的工作和生活上的便利。然而，网络作为一把锋利的双刃剑，它在为科学研究、经济建设、商业活动和日常生活提供高效、经济、方便的同时，也为网络犯罪、计算机病毒提供了生存环境。本章主要介绍网络安全的含义及主要特征、网络安全案例、网络系统的安全威胁与漏洞、网络系统的安全目标及构成要素和网络信息的安全保护等级等内容。通过对本章的学习，读者对网络安全及相关知识会有一个粗略的了解，这对于按计划学好本书后续知识具有重要的指导作用。

1.1　网络安全简介

作为一个开放的网络，Internet 对任何一个具有网络连接和 ISP 账号的人都是开放的，它本身并没有能力保证网络上所传输的信息的安全性，因此 Internet 是不安全的。近年来，随着计算机和网络技术的广泛应用，计算机及网络系统被攻击与破坏的事件不胜枚举。目前，计算机及网络系统安全问题已经引起了世界各国的高度重视，各国不惜投入大量的人力、物力和财力来保障计算机及网络系统的安全。

1.1.1　网络安全的定义

一般意义上讲，安全就是指客观上不存在威胁，主观上不存在恐惧，或者说没有危险和不出事故，不受威胁。就计算机网络系统来说，其安全问题也是如此，就是要保证整个计算机网络系统的硬件、软件及其系统中的数据保护，不受偶然的或者恶意的破坏、更改、泄露，系统连续、可靠、安全地运行，保证网络服务不中断。

由于现代信息系统都是建立在网络基础之上的，网络安全本质上是网络上的信息安全。从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可靠性和可控性等相关的理论和技术都是网络安全研究的领域。因此，网络安全包括网络系统运行的安全、系统信息的安全保护、系统信息传播后的安全和系统信息内容的安全等各方面的内容，即网络安全是对信息系统的安全运行、运行在信息系统中的信息的安全保护（包括信息的保密性、完整性、可用性、可靠性和可控性保护等）、系统信息传播后的安全和系统信息内容的安全的统称。

（1）网络系统运行的安全是信息系统提供有效服务（即可用性）的前提，主要是保证信息处理和传输系统的安全，本质上是保护系统的合法操作和正常运行。其主要涉及计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的安全可靠的运行，计算机操作系统和应用软件的安全，电磁信息泄露的防护等，它侧重于保证系统正常的运行，避免因系

统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁泄露产生信息泄露、干扰他人（或受他人干扰）。

（2）网络系统信息的安全保护主要是确保数据信息的保密性和完整性等，包括用口令鉴别、用户存取权限控制、数据存取权限、方式控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

（3）网络系统信息传播后的安全包括信息过滤技术，它侧重于防止非法、有害信息的传播和控制传播后的后果；避免公用通信网络上大量自由传输信息的失控，本质上是维护道德、法则或国家利益。

（4）网络系统信息内容的安全侧重于网络信息的保密性、真实性和完整性；避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损用户的行为，本质上是保护用户的利益和隐私。

1.1.2 网络安全的主要特征

由前述可知，网络安全主要涉及系统的可靠性、可用性和保密性以及软件和数据的保密性、完整性、可用性、可靠性、可控性和可审查性等。

（1）保密性（Confidentiality）：主要是利用密码技术对软件和数据进行加密处理，保证在系统中存储和在网络上传输的软件和数据不被无关人员使用和识别。

（2）完整性（Integrity）：是指保护网络系统中存储和传输的软件及数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序，数据库中的数据或系统中的程序或数据不被破坏等。

（3）可用性（Availability）：是指在保证软件和数据完整性的同时，还要确保其能被正常使用和操作等。

（4）可靠性（Reliability）：是指保证网络系统不因各种因素的影响而中断正常工作。

（5）可控性（Controllability）：是指网络系统对信息的传播、使用等具有控制能力，可以控制授权范围内的信息流向及方式。

（6）可审查性（Accountability）：是指在网络系统中，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息等。

1.2 网络安全案例与分析

网络安全面临的威胁可以被分成人为和非人为两大类，如图 1-1 所示。当前，网络系统所面临的威胁正随着计算机和网络技术的广泛应用不断增加，因此网络安全事件呈逐年上升趋势。黑客的手段越来越高明，可以利用的黑客工具也越来越多。一些黑客不再需要是计算机高手，他们只要利用网上随处可下载的工具就能轻而易举地对网络发动攻击；而且黑客和病毒技术有融合的趋势。黑客正将病毒作为一种攻击和破坏网络系统的手段，而病毒也将黑客技术引入到病毒之中，使一些程序同时具有了病毒和黑客程序的特征，其危害程度更大。

由于网络信息具有共享性和易于扩散等特性，它在处理、存储、传输和使用上有严重的脆弱性，很容易被泄露、窃取、篡改、假冒、破坏以及被计算机病毒感染。

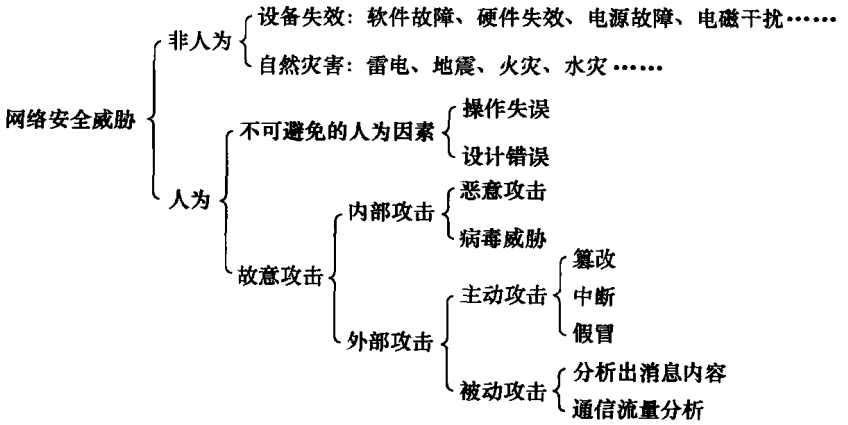


图 1-1　网络安全威胁的分类

1.2.1　网络犯罪案例

1. 国外典型的网络犯罪案例

国外第一例利用计算机网络犯罪案例产生于 1958 年的美国硅谷，但直到 1966 年才被发现，一位计算机工程师通过篡改程序的方式在银行存款余额上做了手脚，这也是世界上第一例受到法律追诉的计算机网络犯罪案。

1983 年，还是学生的 Kevin Poulesn 成功入侵 Arpanet（Internet 的前身）。Kevin Poulesn 当时利用 Arpanet 的一个漏洞，能够暂时控制整个美国的 Arpanet。

1988 年，年仅 23 岁的 Cornell 大学学生 Robert Morris 在 Internet 释放了世界上首个“蠕虫”程序。Robert Morris 最初仅仅是将这个只有 99 行的程序放在 Internet 上进行试验，可结果却使他的电脑被感染而迅速在 Internet 上蔓延开来。美国等地接入 Internet 的计算机受到影响，Robert Morris 也因此于 1990 年被判入狱。

20 世纪 90 年代早期，Kevin Mitnick（一位世界范围内的“超级”黑客）轻而易举地光顾了若干世界上最强大的科技和电信公司的计算机系统，如 Nokia（诺基亚）、Fujitsu（富士通）、Motorola（摩托罗拉）和 Sun Microsystems 等。1995 年，Kevin Mitnick 被 FBI 逮捕，于 2000 年获得假释。Kevin Mitnick 从来没有把自己的这种入侵行为称为黑客行为，按照他自己的解释，他自己的这种入侵行为应为“社会工程（Social Engineering）”。

1993 年，自称为骗局大师（MOD）的组织，将目标锁定美国电话系统。该组织成功入侵美国国家安全局（NSA）、AT&T 和美利坚银行，该组织建立了一个可以绕过长途电话呼叫系统而侵入专线的系统。

1995 年，来自俄罗斯的黑客 Vladimir Levin 在 Internet 上上演了“精彩”的“偷天换日”，他也是历史上第一个通过入侵银行电脑系统来获利的黑客，他成功侵入美国花旗银行并盗走 1000 万美元（他于 1995 年在英国被国际刑警逮捕）。之后，他将账户里的钱转移至美国、荷兰、芬兰、德国、爱尔兰等国家。

1996 年，据美国旧金山计算机安全协会与联邦调查局的一次联合调查统计，有 53%的企业受到过计算机病毒的侵害，有 42%的企业的计算机系统在过去 12 个月内被非法使用过；五角大楼的一个研究小组称美国一年中遭受的攻击就达 25 万次多。

1996年，美国黑客Timothy Loyd将一个仅6行的恶意代码放在其雇主——Omega工程公司（美国航天航空局和美国海军最大的供货商）的网络上，导致Omega公司的所有负责开发生产的软件被删除。此事件导致Omega公司损失1000万美元。

1996年12月29日，黑客入侵美国空军的全球网站并将其主页肆意篡改，其中有关空军的介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言，迫使美国国防部一度关闭了80多个军方网站。

1999年，年仅30岁的David Smith编写的Melissa病毒（是世界上首个具有全球破坏力的病毒）使世界上300多家公司的计算机系统崩溃，整个病毒造成的损失接近4亿美元。随后，David Smith被判处5年有期徒刑。

2000年，年仅15岁的MafiaBoy（由于年龄太小，没有公布其真实身份）在2000年2月14日情人节期间成功入侵包括eBay、Amazon.com和Yahoo在内的大型网站服务器，并成功阻止了服务器向用户提供服务。MafiaBoy也于2000年被捕。

2002年2月，Yahoo网站、Amazon.com和ZDNet遭遇分布式拒绝服务攻击。

2002年11月，英国人Gary McKinnon被指控非法入侵美国军方90多个计算机系统，随后被引渡到美国受审。

2005年，英国一名受雇于人的黑客贾斯明·辛，使用DoS攻击企图彻底打垮对手的在线销售网点。他利用计算机病毒控制上千台计算机，组成了傀儡网络，向两家在线销售体育服装的公司网站发起DoS攻击，并成功窃取大量信息。

2005年，韩国一名未满17岁的少年，使用“黑客软件”获取他人密码之后，从受害人银行账户中转走5000万韩元（约5万美元）。

2007年6月21日，美国国防部部长亲口证实，五角大楼的一个非保密电子邮件系统一天前遭黑客攻击，迫使国防部1500个邮件账户被停机使用，一至于美国众议员兰吉在国土安全委员会听证会上忧心忡忡地说:“这说明什么？这意味着恐怖分子或其他国家入侵美国国土安全部的数据库，篡改姓名以便让他们能够进入我国，而我们根本不晓得他们已经得逞!”

2007年6月22日，正当全球无数哈利·波特迷热切期盼《哈利·波特》系列小说的大结局面世时，一名计算机黑客突然对外宣称，他已经成功闯入了出版商的计算机系统盗走了文稿，并且将部分内容粘贴在Internet上。

2007年9月2日，美国宣布美国政府招聘人员专用网站遭受黑客攻击，大约14.6万名用户数据被盗，以至于网站随即被关闭。

2008年，美国东海岸连锁超市（East Coast）的母公司Hannaford Bros.称，该超市的用户数据库系统遭到黑客入侵，造成400多万个银行卡账户信息泄露，因此导致了1800起与银行卡有关的欺诈事件。在持卡人认证过程中，有420万个单个的信用卡和借记卡信息泄露，成为迄今为止涉及用户规模最大的数据入侵事件之一。

2008年，在俄罗斯向格鲁吉亚发动战争前，格鲁吉亚社会基础网络便受到了俄罗斯黑客的攻击。接下来，几乎与战争同步，格鲁吉亚政府网站也遭到了黑客攻击。格总统萨卡什维利的个人主页被人篡改，宣称“萨卡什维利与希特勒有某些‘共同之处’”的照片被放在首页上。迫于无奈，8月10日，格鲁吉亚方面把总统的网站从格鲁吉亚境内的服务器迁到了美国的服务器上。俄罗斯方面则表示，来自格鲁吉亚的黑客攻击了俄方的新闻机构。

2009年4月，一个17岁的高中生（Michael Mooney，其黑客名为Mikeyy）在Twitter上传播一种流行蠕虫病毒，导致该公司不得不至少删除了可继续传播病毒的190个失密账户、

10 000 个感染的 Tweets 用户。

2010 年 8 月 11 日，美联邦特工逮捕反抗美帝国主义的莫斯科黑客弗拉季拉夫·霍罗霍林。根据报道霍罗霍林（网络绰号为“BadB”）是全球最危险、最精明的五大网络犯罪分子之一，拥有以色列和乌克兰国籍，长期定居莫斯科，通过创建的黑客网络，霍罗霍林及其同伙实施了几乎是美国历史上规模最大的金融信息盗窃案。

2. 国内典型的网络犯罪案例

1986 年 7 月 22 日，港商李某在深圳某银行取款时，发现账户上 2 万元不翼而飞，而两个月后，同样在深圳，赵某存入银行的 3 万元港币也从户头离奇蒸发（而此案破获后，上述两笔款项均为同一犯罪分子利用计算机知识诈骗而去，这也是国内第一起利用计算机网络犯罪案例）。

1996 年，中科院高能物理所遭到入侵，黑客私自在高能所的主机上建立了几十个账户，经追踪发现是由国内某拨号上网用户所为。

1996 年 2 月，刚开通不久的 CHINANET 受到黑客攻击，而且黑客攻击得逞。

1997 年 4 月 23 日，美国德克萨斯州内查德逊地区的西南贝尔互联网公司的 PPP 用户入侵中国互联网信息中心的服务器，并破译了该系统的 shutdown 账户，并将中国互联网信息中心的主页换成了笑嘻嘻的骷髅图像。

1998 年 2 月，广州视聆通被黑客多次入侵，造成 4 小时的系统失控。

1998 年 4 月，贵州信息港被黑客入侵，主页被一幅淫秽图片替换。

1998 年 5 月，大连 ChinaNET 节点被入侵，用户口令被盗。

1998 年 6 月，上海某信息网被入侵，多台服务器的管理员口令被盗，数百个用户和工作人员的账号、密码被窃取，7 月 13 日，犯罪嫌疑人杨某被逮捕.这是我国第一例电脑黑客事件（当时 22 岁的杨某是国内一著名高校数学研究所计算数学专业的直升研究生，具有国家计算机软件高级程序员资格证书，具有相当高的计算机技术技能。据说，他进行电脑犯罪的历史可追溯到 1996 年，当时，杨某借助某高校校园网攻击了某科技网并获得成功.此后，杨某又利用为一电脑公司工作的机会，进入上海某信息网络，其间仅非法使用时间就达 2000 多小时，造成这一网络直接经济损失高达 1.6 万元人民币。

1998 年 7 月，江西 169 网被黑客攻击，造成该网 3 天内中断运行 2 次。

1998 年 8 月，西安某银行被黑客攻击，并被盗取 80.6 万元。

1998 年 9 月，扬州某银行被黑客攻击，利用虚存账号提走 26 万元现金。

1998 年 10 月，福建省图书馆主页被黑客替换。

1999 年元旦刚过，来自美国佛罗里达州等地号称自己是“地下军团”的一批黑客向中国政府的一些网站发起攻击：1 月 2 日，北京一家 ISP（国网，被误解为国家网）报告网页被黑客替换；1 月 4 日，某地区的中经网连续三次网页被篡改，且系统账号被封；1 月 7 日，中国财政部的网站被黑客攻击；1 月 8 日，“中国之窗”（国外站点）也遭黑客殃及；1 月 9 日，“中国人权”网站的主页被替换。

1999 年 1 月底，广东首宗电脑“黑客”伪造车票案告破，涉案金额约合人民币 445 万元。

1999 年 10 月 25 日中央电视台报道，我国首起证券市场电脑“黑客”案日前告破，黑客造成某证券公司损失 300 多万元。

1999 年 8 月，由于李登辉的“两国论”激怒了中国黑客，中国台湾省的数十个网站被

攻击。

2000 年 2 月 28 日，河北省邯郸电信局“邯郸信息港”主页被篡改，经公安机关调查，作案人系该市一高中生。

2001 年 1 月 30 日 1 点钟左右，263 网络集团的 ISP 业务页面、IDC 资料信息港页面等几乎在同一时刻被黑客攻击。

2001 年 2 月，武汉邮电科学研究院被黑，首页页头被加上“这里是信息产业部邮科院的网站，但已经被黑”的字样。

2001 年 2 月 20 日，通港网络（中国电信）、北京电信发展总公司、北京移动、北京寻呼、中国地图出版社、华建集团等 40 余家网站被黑，其大面积的攻击让国内网站再一次感受到网络安全问题的严重性。

2001 年 5 月 17 日，长沙破获首例“黑客”攻击网吧案，黑客是利用了国内的一个黑客工具对 OICQ 进行攻击，致使一网吧停业三天；5 月 30 日，北京某大学生利用网上下载的黑客软件进入某网站，盗取了一公司的上网账号和密码并且散发，致使该公司经济损失 40 多万元。

2002 年，福建首例黑客“入侵、破坏交警计算机网络”，造成驾驶员违章记录被删除，交警电脑网络信息、数据程序被删改（2003 年 1 月此案在泉州被告破）。

2003 年 1 月 25 日，中国互联网遭到大面积蠕虫病毒感染，部分瘫痪，直到晚上九点半，该安全事件才得到初步控制（中国 80%以上网民受此次全球性病毒袭击影响而不能上网，很多企业的服务器被此病毒感染引起网络瘫痪）。

2003 年 4 月发生在江苏无锡的一起盗买盗卖股票案件，盗取被害人资金账号及交易密码后，以高吃低抛某一股票，同时在自己的资金账号上低吃高抛同一股票的方法，给被害人造成 37.1 万余元的经济损失，从中非法获利 19.8 万余元。

2003 年 7 月，“传奇 3”连续三天遭到黑客大规模有预谋、有组织、持续的攻击，“传奇 3”部分服务器端口被堵死，致使玩家不能进入（其中“神话”服务器专区的情况最为严重，致使光通被迫对该区进行停机维护），这也是黑客第一次对一个游戏运营商实施这样大规模的攻击。

2003 年 8 月，一种名为“冲击波”（Blaster）的新型蠕虫病毒开始在国内互联网和部分专用信息网络上传播（该病毒传播速度快、波及范围广，对计算机正常使用和网络运行造成严重影响。这是网络病毒袭击微软程序的所有行动中造成的后果最严重的一次）。

2004 年中国网络安全工作报告显示，CNCERT/CC 在 2004 年共收到国内外通过应急热线、网站、电子邮件等报告的网络安全事件 64 686 件（同 2003 年全年收到 1 万 3 千多件报告数量相比，2004 年网络安全事件报告数量大大增加），CNCERT/CC 处理了 200 多起针对银行等机构的跨国互联网仿冒欺诈（Phishing）事件，我国大陆地区 6 600 多个 IP 地址的主机被植入木马。

2005 年，中国台湾地区一名 38 岁的无业男子，破解了中国台湾地区 40 多家网络银行的虚拟键盘，取得上千笔资料，并冒充银行发送网络钓鱼 E-mail，到处散播伪造的第二代金融卡驱动升级程序。

2006 年 10 月，成都某高校电子商务专业 03 级在校大学生宋某在成都市利用互联网多次搜索他人身份证号码和招商银行卡卡号，并提供身份证测试银行卡密码，最终在测试成功后，通过网上消费等方法，窃取苏州某高校在校 44 名大学生发放奖学金的银行卡内的存款

51 619.12 元。

2007 年，以手拿 3 支香的熊猫图标为代表的“熊猫烧香”病毒攻击了数千网站（其中不乏金融、税务、能源等关系到国计民生的重要单位），而受到攻击的个人用户更不下千万，其危害程度不亚于 CIH、震荡波、冲击波等老牌计算机病毒。

2008 年，中国警方破获的最大一起网络黑客犯罪案件中，犯罪嫌疑人就是利用一款名为“大小姐”的木马病毒来盗取他人游戏账号（这个“大小姐”木马程序可以针对 40 多款网络游戏进行盗号，担负老板角色的犯罪嫌疑人王某通过这个木马，非法获利 1400 余万元），如此疯狂地作案并且屡屡得手，使得“大小姐”木马在这个产业链当中，竟有了品牌效应。

2009 年，瑞星推出“恶意网站监测网”（http://mwm.rising.com.cn/，这是国内首个专门针对挂马网站、钓鱼网站等互联网威胁的实时监测系统）显示， 6 月 9 日互联网上共有 42 万个网页带有木马活动，118 万人次网民遭受攻击。

2009 年 5 月 19 日，江苏、安徽等 6 省区出现罕见的断网事件，大量网民无法正常访问网站。断网事件背后的一个犯罪事实是：部分商家为打击竞争对手，雇用黑客发动网络攻击。而这些黑客通常会挟持大量被感染病毒的电脑，即所谓的“肉鸡”，一起发动大规模黑客攻击。这次断网事件祸起网络游戏“私服”市场。“私服”因利益纠葛，相互火并的现象极为普遍，一些实力雄厚的“私服”甚至每月都会花费两三百万元打击竞争对手。

2010 年 1 月，湖北仙桃市的“1·22”大学生网络犯罪案，导致该市公安局的大部分计算机瘫痪。据犯罪人嫌疑人交代，他们还利用“熊猫烧香”病毒将几种病毒合并在一起，演变成一种新病毒“肉鸡”来控制电脑，在电脑里制造木马程序，盗窃他人电脑里的 QQ 号、游戏装备等，得手后变卖获利。

2010 年 3 月 17 日，黑龙江省牡丹江市公安机关摧毁一个网银诈骗犯罪团伙。经查，2009 年 11 月以来，犯罪嫌疑人姜某伪造某银行网站，并诱使被害人在该网站上填写网银用户名、密码等，随后冒用被害人的名义，通过网上银行盗取银行卡内资金。

1.2.2　网络犯罪活动分析

由前面的网络犯罪案例可以看出，近年来网络犯罪案件数量呈逐年上升的趋势，其中利用病毒等恶意代码窃取用户信息、敲诈用户财产成为网络犯罪的主要手段之一，同时，网上贩卖病毒、木马和僵尸网络的活动不断增多且公开化。利用病毒、木马技术传播垃圾邮件和进行网络攻击、破坏的事件呈上升趋势。因此，种种迹象表明，病毒的制造、传播者追求经济利益的目的越来越强，这种趋利性引发了大量的网络犯罪活动，危及网络的应用与发展。

1. 智能化的特点

计算机病毒犯罪是一种高智能的犯罪，更需要的是知识和技术或者说是脑力，而不仅仅是需要暴力和凶残。犯罪分子往往不仅懂得如何操作计算机的指令和数据，而且还会编制一定的程序，解读或骗取他人计算机的口令密码。

2. 网络化的特点

计算机病毒犯罪网络化特点明显，利用计算机病毒犯罪不受时间地点限制，犯罪行为的

实施地和犯罪后果的现地可以是分离的，甚至可以相隔十万八千里。而且受害者一旦感染病毒，犯罪分子可以随时盗取其计算机内的重要信息。比如：犯罪分子在北京，而其挂马的服务器在上海，受害人则有可能在广州。这样充分利用了网络没有空间和时间限制的特点，给侦破工作带来极大难度。

3. 隐蔽性的特点

隐蔽性包括两方面：一方面任何恶意代码都希望在被感染的计算机中隐藏起来不被发现，因为只有在不被发现的情况下，才能长期实施其破坏行为。为了达到这个目的，许多病毒使用了各种不同的技术来躲避反病毒软件的检验。另一方面，由于近几年对于网上木马的严厉打击，木马病毒等恶意程序制作者已成了惊弓之鸟，作案后很少还会留下蛛丝马迹，这给网络犯罪取证工作也带来了巨大困难。

（1）网络犯罪分子抓住网络存在的技术漏洞和人们安全防范意识不强的环节，利用病毒、木马等黑客技术和网络欺诈手段，具有极强的隐蔽性。犯罪分子利用的木马和病毒，对被感染的计算机系统影响越来越小，感染后几乎没有明显的特征，木马或病毒在机器中潜伏几个月甚至几年都有可能不被发现。当受害者发现网络银行或者重要信息被盗时，犯罪分子早就毁灭证据，逃之夭夭了。

（2）网络犯罪分子在网络一般都使用虚拟身份，并且使用网络通讯工具进行联系，犯罪分子之间也没有见过面，这使得很难确定其在现实生活中的真实身份。充分利用“虚拟社会”的特点，给犯罪分子的抓获带来了极大的麻烦。

4. 网上木马贩卖公开化，泛滥严重

网上木马贩卖情况有愈演愈烈之势，在互联网上以“木马”、“贩卖木马”或者“黑客”等为关键字可以搜索出十几万条相关信息。网上充斥着大量的关于木马、黑客和病毒的信息。在众多网站、论坛和博客上，公开发布贩卖木马的相关信息，甚至可以轻易地从网络上获取到大量的木马病毒和黑客工具等恶意程序。

5. 集团化、产业化的趋势

目前的病毒犯罪早已摆脱了独立的散兵游勇状的个人行为，而转变为并不严密但却绝对保密的小集团性质的集体行为，犯罪团伙组成有十到上百人不等。从近期破获的几起病毒案来看，病毒团伙成员分工明确，组织严密，各司其职，人员数量庞大，逐渐形成了明显的病毒产业链：病毒木马编写者→专业盗号人员→销售渠道→最终玩家。

6. 作案成本低，办案成本高

计算机病毒犯罪案件作案时间短、过程简单，可以单独行动，而且犯罪工具很容易获得，犯罪分子很容易就可以在网上下载或者购买相关的木马或病毒。存在目击者的可能性很少，而且即使有作案痕迹，也可被轻易销毁，发现和侦破都十分困难。如例用黑客程序的犯罪，只要几封电子邮件，被攻击者一打开，就完成了，因此，不少犯罪分子越来越喜欢用互联网来实施犯罪，只需要坐在电脑旁，动动手指就能使资金往来。与此相反，公安机关只能采用跨地域侦查取证的办案方式，成本高、效率低。

7. 国外势力、敌对势力逐步渗透黑客组织企图破坏网络稳定

通过对网络上黑客组织的调查，有迹象表明国外势力、敌对势力等正在通过各种渠道和国内的黑客进行联系，企图通过各种手段进行拉拢收买为其所用，并且出高价购买国内黑客制作的各种木马和病毒，有可能会对互联网的安全稳定带来严重的威胁。

8. DDoS 攻击可能成为网络犯罪的主要手段

DDoS 会对目标网络发起拒绝服务攻击，攻击者虽然没有直接获得利益，但攻击者可以令目标服务商减少收益或增加成本。从近期破获的一些案例中，可以总结出 DDoS 有以下几种犯罪方法。

（1）网络黑社会的打劫。发现某家网站经营业绩好，黑客就会向该家网站收取所谓的“保护费”，如果不给，就用 DDoS 对其网站进行攻击，造成该网站网络瘫痪，给其经营者造成重大损失。很多经营者无力解决这些问题，只好将保护费拱手送上。

（2）网络敲诈。某些不太合法，但收益还不错的网站，会成为黑客利用 DDoS 攻击的重点目标。比如，某些色情网站、赌博网站和网络游戏的私服等。这些网站即使被攻击了也不敢向警方报案，只能向黑客妥协。

（3）网络恐怖组织。国外势力、敌对势力很可能会利用其控制的僵尸网络，在某一敏感时期或重要活动期间，对国内重要单位网站或重要网络节点进行 DDoS 攻击，造成大规模网络瘫痪，形成网络恐慌，严重影响国内网络安全。

1.3　网络系统的安全威胁与漏洞

1.2 节中的网络安全案例说明，黑客攻击的手段五花八门，攻击的目的也各不相同。目前，网络病毒在全球范围内仍在不断扩散，网络黑客攻击事件与日俱增；随着网络应用技术的不断更新与发展，黑客攻击技术与网络病毒日趋融合，并成为目前网络攻击发展的趋势。近年来，随着网络攻击工具的日益先进，攻击者需要的技能日趋下降，网络受到攻击的可能性也越来越大。因此，在开放自由的 Internet 环境中，没有绝对安全的网络信息系统，网络安全隐患无处不在，有的甚至是不堪一击的。

1.3.1　网络系统的安全威胁

众所周知，Internet 在推动社会发展的同时，也面临着日益严重的安全问题。目前，网络安全威胁主要来自物理风险、网络风险、系统风险、信息风险、应用风险、管理风险和其他风险等。这些风险主要来自计算机病毒、系统内部和外部的攻击、信息存储安全、信息传输安全、信息访问安全等。

（1）物理风险：主要涉及设备的防盗及防毁、线路老化及人为破坏（包括被动物咬断）、网络设备自身故障、停电导致网络设备无法正常工作、机房电磁辐射及其他等方面。

（2）网络风险：主要涉及网络系统的安全拓扑、安全路由及其他等方面。

（3）系统风险：主要涉及自主版权的操作系统、操作系统是否安装最新补丁或者修正程序、安全数据库、系统配置安全、系统运行中的服务安全及其他等方面。

（4）信息风险：主要涉及信息存储安全、信息传输安全、信息访问安全及其他方面等。

（5）应用风险：主要涉及身份鉴别、访问授权、机密性、完整性、不可否认性、可用性及其他等方面。

（6）管理风险：主要涉及是否制定了健全完善的信息安全制度、是否成立了专门的机构来规范和管理信息安全及其他等方面。

（7）其他风险：主要涉及计算机病毒、网络黑客攻击、误操作导致数据被删除及修改、其他没有想到的风险等。

1.3.2 网络信息系统的漏洞及弱点

由于现有的操作系统（无论是 Unix/Linux，还是 Windows）都存在种种安全隐患，每种系统都存在已被发现和潜在的各种安全漏洞，导致非法用户可以获得系统的访问权、合法用户未经授权提高访问权限等。在当前使用最为广泛的 Internet 服务中，都不可避免地存在这样或那样的漏洞。比如，电子邮件中的匿名信、冒名邮件及大量涌入的垃圾邮件；再比如，FTP 站点中的隐藏的病毒威胁等。目前，常见的漏洞主要有网络协议的安全漏洞、操作系统的安全漏洞和应用程序的安全漏洞等 3 类。

1. 网络信息系统安全漏洞产生的原因

网络信息系统安全漏洞产生的原因很多，但主要体现在以下几方面。

（1）配置管理和使用不当产生的安全漏洞，比如系统口令过于简单，很容易被黑客猜中。

（2）技术实现不充分产生的安全漏洞，比如很多缓冲区溢出方面的漏洞就是在实现时缺少必要的检测而带来的安全威胁。

（3）系统和软件的设计存在缺陷，比如在设计系统和软件时考虑不充分，导致在使用中被黑客所利用，引发诸多安全事件。

（4）通信协议不完备，比如 TCP/IP 存在诸多缺陷和很多漏洞。

2. 网络信息系统漏洞造成的危害等级

当前，由于系统漏洞引发的安全事件受到了广泛关注，不同的漏洞所带来的危害程度也不尽相同。一般而言，按照对目标（主机或系统）的危险程度，漏洞可分为以下三级。

（1）A 级漏洞：允许恶意入侵者访问，并可能会破坏整个目标系统的漏洞。

（2）B 级漏洞：允许本地用户提高访问权限，并可能使其获得系统控制的漏洞。

（3）C 级漏洞：允许用户中断、降低或阻碍系统操作的漏洞。

3. 从信息处理过程的角度看网络信息系统的弱点

在目前的网络系统中，信息在其整个生命周期中都存在相应的弱点，黑客往往利用这些弱点进行黑客任务，从而造成诸如以下的信息安全事件。

（1）信息存储安全。信息存储安全是指信息在静态存储状态下的安全，其主要弱点表现在磁盘、光盘意外损坏及存储设备被盗等，从而造成数据丢失和数据无法访问等。

（2）信息传输安全。信息传输安全是指信息在动态传输过程中的安全，其主要弱点表现在诸如攻击者的搭线窃听和重放攻击等，从而造成信息泄露和信息被篡改。