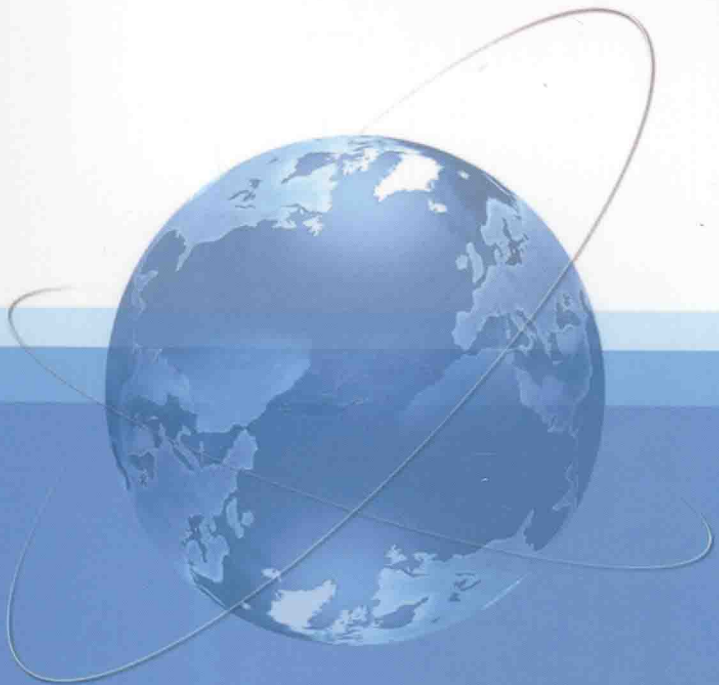
高等职业教育“十二五”规划教材

21世纪高职高专规划教材

（计算机类）

网络安全技术



第2版

陈卓　主编

机械工业出版社
CHINA MACHINE PRESS

配多媒体课件

高等职业教育“十二五”规划教材
21世纪高职高专规划教材（计算机类）

网络安全技术

第2版

主　编　湖北工业大学　陈　卓
副主编　黄冈职业技术学院　蔡向阳
山东日照职业技术学院　唐海和
参　编　黄冈职业技术学院　陈金莲
湖北交通职业技术学院　刘　桥

机械工业出版社

本书在第1版的基础上进行了修改和完善，全面介绍了网络安全的基本概念、原理以及应用，主要内容包括密码算法基础、身份认证技术、黑客攻击与防范、计算机病毒的原理与防御、防火墙技术及应用、入侵检测技术、操作系统安全、数据的备份与恢复，最后介绍了网络安全系统的规划与设计。

本书根据高职高专计算机网络技术专业的要求编写，并考虑了计算机相关专业的要求，内容丰富，文字浅显易懂，可作为高职高专计算机网络以及计算机应用等专业的教材，也可作为计算机爱好者的自学参考书。

为方便教学，本书配备电子课件等教学资源。凡选用本书作为教材的教师均可登录机械工业出版社教材服务网www. cmpedu. com注册后免费下载。如有问题请致信cmpgaozhi@ sina. com，或致电010-88379375联系营销人员。

图书在版编目(CIP)数据

网络安全技术/陈卓主编. —2版. —北京：机械工业出版社，2012.5
21世纪高职高专规划教材　高等职业教育“十二五”规划教材. 计算机类
ISBN 978-7-111-37925-6

Ⅰ. ①网…　Ⅱ. ①陈…　Ⅲ. ①计算机网络-安全技术-高等职业教育-教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2012）第059505号

机械工业出版社(北京市百万庄大街22号　邮政编码100037)
策划编辑：余茂祚　责任编辑：余茂祚　罗子超
版式设计：霍永明　责任校对：潘　蕊
封面设计：马精明　责任印制：杨　曦
北京圣夫亚美印刷有限公司印刷
2012年6月第2版第1次印刷
184mm×260mm　·13.75印张·339千字
0001—3000册
标准书号：ISBN 978-7-111-37925-6
定价：26.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
电话服务　　网络服务
社服务中心　：(010)88361066　门户网：http://www. cmpbook. com
销售一部　：(010)68326294　教材网：http://www. cmpedu. com
销售二部　：(010)88379649　**封面无防伪标均为盗版**
读者购书热线：(010)88379203

21世纪高职高专规划教材

编委会名单

前　言

在信息技术飞速发展的今天，网络安全关系到国家的主权和安全，这是一个必须正视的问题。因此，构筑面向21世纪的国家信息安全保障体系，无疑具有十分重要的战略意义。

时代需要网络，网络需要安全。

在2004年7月召开的“全国高校本科信息安全规范与发展战略研究”成果发布与研讨会，给出了信息安全专业战略发展与规范的两个主要文件：一是信息安全学科专业发展战略研究，二是全国高校本科信息安全专业规范，指出信息安全专业人才至少应当包括研究性或学术性的信息安全专业人才（主要以研究性大学和教学研究型大学为培养主体）、应用型的信息安全人才（主要以教学主导型培养主体，技术型）和职业型的信息安全人才（以高等职业院校为主体）。由此可见，职业型信息安全人才是我们国家信息安全人才培养的重要组成部分。在社会面临日益严重的网络安全问题的大背景下，国家和各行业对网络安全人才的需求日趋旺盛，而真正具备足够理论知识和实战经验的网络安全人才却不多，远远不能满足社会需求。因此，培养高质量的职业型信息安全人才是高等职业院校义不容辞的责任。

网络安全涉及的理论比较生涩难懂，可能这是初入此道者翻了几本书后的共同心理。正是在这种情况下，我们根据高职高专计算机网络技术专业的需要，并考虑了计算机专业及相关专业的要求，编写了本书。本书力求以通俗的语言和清晰的叙述方法，向读者介绍计算机网络安全的基本理论和常用的安全技术。

《网络安全技术》一书自从2004年8月由机械工业出版社出版以来，多次重印，很受读者的欢迎。经过编者精心修订的第2版教材具有如下特色：

（1）知识实用、丰富、新颖

网络的发展日新月异，编者在教学过程中也深感网络安全技术在飞速发展，相关网络安全的新的理论和新的技术能够适时补充到原有教材是十分必要的，作为第2版，本书保留了原书的风格和基本体系，增加了身份认证技术、黑客攻击与防御、数据备份与恢复、网络安全系统设计规划这4个章节，并对原有章节进行了内容的更新，比较第1版，第2版更全面地反映网络安全的最新技术。

（2）强调实践性

网络安全技术实践性很强，仅仅通过书本，学生不可能全面深入地掌握网络安全的知识体系，更不可能在未来工作的网络安全攻防竞争中处于优势地位，对于高职高专的学生尤其如此。网络安全的实验教学近年来一直是国内网络安全教学的探索方向，本书中增加了更多的验证性实验，补充了一些综合性实验，增加了网络安全实践工程实例的内容比例，并详细介绍了操作步骤，使全书内容更具有实用性。

本书内容共分10章。

第1章为计算机网络安全概述，主要介绍了计算机网络安全的定义、计算机网络面临的

主要威胁，网络安全的基本需求：机密性、完整性、可用性、不可否认性等，以及构建网络安全体系结构的主要技术、网络安全的级别分类和我国网络安全现状。

第2章介绍密码学的历史与发展、密码学的基本概念、密码算法的分类，学习几种有代表性的古典密码，还介绍了对称密码算法和非对称密码算法的原理与应用。

第3章介绍几种常见的身份认证技术：口令机制、数字证书、智能卡身份认证、基于生物特征识别的身份认证技术。

第4章介绍黑客攻击的原理和针对黑客攻击的防御知识。

第5章介绍计算机病毒的特性、传播途径以及病毒的预防和查杀的知识。

第6章介绍防火墙技术的基本原理、分类以及应用。

第7章介绍入侵检测技术的定义、功能、分类及应用。

第8章主要介绍了以Windows操作系统安全机制为应用背景的操作系统安全。

第9章主要介绍数据备份的基本概念、数据备份方案设计及实施、数据容灾技术以及几种常用的数据备份与恢复工具的使用。

最后，第10章主要介绍网络安全系统规划设计的基本方法以及网络安全平台搭建案例分析。

每章内容后都附有本章小结和复习思考题，帮助读者掌握基本理论和关键技术，同时每章还附有实践与训练，帮助读者学以致用，尽快进入实用状态。

本书参考学时为70学时。建议理论教学40学时、上机教学30学时。教师可以根据学校的教学条件、自己的专业特长和教学需要，适当补充或删减一些教学内容。

本书中介绍的软件大多可以从网上官方免费下载，这样既方便教师教学，也方便学生自学。如果学校条件允许，也可补充介绍一些商业软件、硬件或补充其他一些专业的网络安全教学软件，这样教学效果会更好。

有关本书的电子课件、习题参考答案、部分书中使用的工具软件将放在机械工业出版社教学资源网站（www.cmpedu.com）上，在电子课件中将对书中每章的教学重点、教学要求详细说明，供教师和学生参考。教师课堂教学时，建议多媒体课件、板书相结合，如果教学条件允许，对于有些实践性较强的章节，如果能在机房采用教师演示、学生通过实验验证，可能教学效果会更好。

本书第1、2、3章由陈卓编写，第4章和第5章由陈卓、唐海和共同编写，第6章和第7章由陈金莲编写，第8章和第9章由蔡向阳编写，第10章由刘桥编写。陈卓作为主编对全书进行了统编和最后定稿。

在向读者们热情推荐本书的同时，我们也深深感到计算机网络安全的理论、技术以及应用可谓博大精深，网络安全新技术如雨后春笋，书中如有错误和疏漏，敬请各位读者批评指正，并提出宝贵意见。

编　者

21 世纪高职高专规划教材书目（基础课及电和计算机类）

（有*的为普通高等教育“十一五”国家级规划教材并配有电子课件）

*高等数学（理工科用） 第2版
高等数学学习指导书（理工科用） 第2版
计算机应用基础 第2版
应用文写作
应用文写作教程
经济法概论
法律基础
法律基础概论
*C 语言程序设计

工程制图（非机械类用）
工程制图习题集（非机械类用）
离散数学
电工电子基础
电路基础
单片机原理与应用
电力拖动与控制
*可编程序控制器及其应用（欧姆龙型）
可编程序控制器及其应用（三菱型）
工厂供电
微机原理与应用

模拟电子技术
*数字电子技术
数字逻辑电路
*办公自动化技术
现代检测技术与仪器仪表
传感器与检测技术
*制冷原理与设备
制冷与空调装置自动控制技术
电视机原理与维修
自动控制原理与系统
电路与模拟电子技术
低频电子线路
电路分析基础
常用电子元器件
单片机原理及接口技术案例教程
多媒体技术及其应用操作系统
*数据结构
数据库基础及其应用
数据库设计及其应用
软件工程
微型计算机维护技术
汇编语言程序设计

VB6.0 程序设计
VB6.0 程序设计实训教程
Java 程序设计
*C++程序设计
Delphi 程序设计
计算机网络技术
网络应用技术
网络数据库技术
网络操作系统
网络安全技术 第2版
网络营销
网络综合布线
网络工程实训教程
*计算机网络技术实验实训指导

计算机图形学实用教程
*三维动画制作
*动画设计与制作
管理信息系统
电工与电子实验
专业英语（电类用）
计算机专业英语

目　录

第1章
计算机网络安全概述

学习目标：

通过本章的学习，要求了解计算机网络安全的定义、面临的主要威胁，掌握计算机网络安全的基本需求：机密性、完整性、可用性、不可否认性等，了解构建网络安全体系结构的主要技术、网络安全级别划分、我国网络安全现状，最后，需要了解网络安全的法律法规，并自觉遵守。

引例：

信息技术的迅猛发展使得计算机网络这一人类伟大的发明已经广泛地深入到社会的各个角落，人们利用网络存储数据、处理图像、互发电子邮件等，充分地享用网络带来的无可比拟的功能和智慧。计算机网络已经成为社会发展进步的重要标志，它的应用遍及国家的政府、军事、科技、文教等领域。其中，存储、传输和加工处理的信息有许多涉及政府宏观调控决策、商业经济信息、银行资金、股票证券、能源资源、科研数据等重要内容。

与此同时，无情的事实表明，除非我们把计算机锁在一个密闭的房间里，并且没有任何计算机与之相连，使其对外界的访问受到隔离，否则该计算机系统就会时刻处于危险之中，随时都可能面临黑客的攻击、少数网民的恶作剧以及个别居心叵测分子的作祟。

近年来，计算机犯罪案件急剧上升，各国的网络系统面临着很大的威胁，并成为严重的社会问题之一。更多职业化黑客的出现，使网络攻击更加有目的性，黑客们已经不再满足于简单、虚无缥缈的名誉追求，更多的攻击背后是丰厚的经济利益。据美国联邦调查局的统计，美国每年因网络安全造成的损失高达上百亿美元。

1.1 引言

1.1.1 计算机网络安全的定义

当你遨游在 Internet 浩瀚无际的信息海洋时，你就会发现计算机只有同网络相连，才是

名副其实的计算机，从一定意义上讲，“网络就是计算机”，“计算机就是网络”，两者密不可分。随着计算机网络的飞速发展，这一关于计算机的现代理念已经越来越得到人们的认可。因此，要给计算机网络安全下定义，首先要了解“计算机安全”的概念。

国际标准化组织（ISO）将“计算机安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，此定义偏重于静态信息的保护。

也曾有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

综合上述计算机安全的定义以及计算机和网络的密切关系，我们可以给“计算机网络安全”作如下定义：“保护计算机网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，保障系统连续可靠地正常运行，网络服务不中断。”

1.1.2 计算机网络面临的安全威胁

为什么计算机网络如此容易受到侵害？主要存在于两个方面的问题：一方面，资源共享是计算机网络的重要特点，这对于无数的计算机用户无疑是好事，否则，网络也不会受到人们如此的青睐。但也正是因为“共享”，容易被一些别有用心者钻了空子，使得网络信息及网络设备的安全受到了种种不同程度的威胁。

另一方面，从网络协议结构设计看，如今使用最广泛的网络协议是 TCP/IP，它是在资源管理及网络技术均不成熟的情况下设计的。它的最初的主要设计目标是互联、互通、共享，而不是安全。实践证明，该协议中已被发现有许多安全漏洞和隐患，这是因为研制者在设计之初并没有过多考虑网络的安全性能。因此，计算机技术，包括网络技术，虽然已经从过去的研究阶段进入了商品实用阶段，但是它的技术基础是不安全的，有其脆弱的一面，这是我们不可否认的客观事实。

知己知彼，百战不殆。下面我们通过计算机网络上两个用户的通信来考察一下网络面临的主要威胁。

（1）截获　发送方通过网络与接收方通信时，如果不采取任何保密措施，那么其他人就有可能截获并偷看到他们的通信内容，如图 1-1 所示。

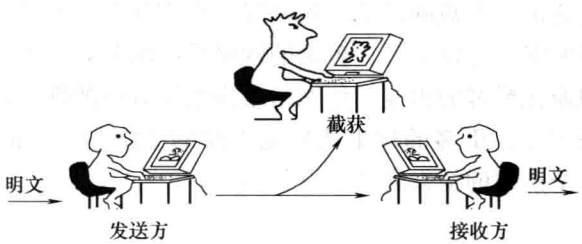


图 1-1　消息被截获

（2）篡改　授权方不仅获得了访问而且篡改了内容。例如，将一笔电子交易的金额由 100 万元改成 1000 万元，比泄露这笔交易本身的结果更严重，如图 1-2 所示。篡改信息包

括对重要文件的修改、更换、删除等，是一种很恶劣的攻击行为，不真实的信息将对用户造成很大的损失。

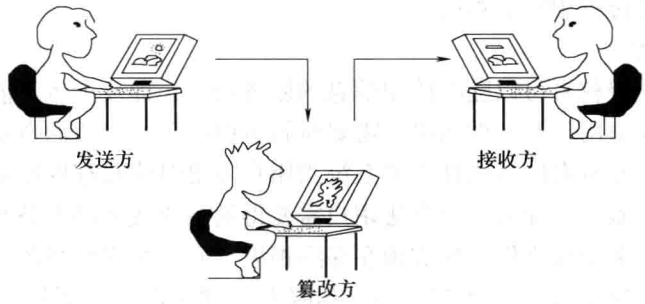


图 1-2 消息被篡改

（3）抵赖 这是通信双方之间可能发生的安全隐患。例如，由于价格行情发生改变，A 否认自己曾经与 B 签署的电子合同。在电子商务系统中特别需要提供抗抵赖服务。

（4）恶意代码 恶意代码包括计算机病毒、“流氓”软件、钓鱼网络以及其他后门程序。其中，计算机病毒是计算机网络面临的主要威胁之一。由于网络的设计目标是资源共享，所以网络是计算机病毒滋生的理想家园。Internet 的发展，大大地加速了病毒的传播速度。

（5）拒绝服务 拒绝服务（Denial of Service，DoS）是一种破坏性的黑客攻击方式，其目的旨在使目的主机陷入停顿或无意义的繁忙，从而使合法用户无法正常使用资源，造成网络效率降低甚至瘫痪。例如，Ping 风暴是一种常用的 DoS 攻击方法，只要多人约定在某个时刻同时对目标主机使用 Ping 程序，就可能耗尽目标主机的网络带宽和处理能力，造成网络效率急剧降低或瘫痪。

（6）欺骗攻击 网络欺骗攻击的主要方式有网络互连协议（IP）欺骗、地址解析协议（ARP）欺骗、域名系统（DNS）欺骗、Web 欺骗等。

1.1.3 计算机网络安全的基本需求

面对计算机网络面临的威胁，人们对计算机网络中的数据安全提出了以下安全需求。

1. 数据的机密性

首先人们意识到的是信息保密。在传统信息环境中，普通人通过邮政系统发送信件，为了个人隐私还要装上信封。可是到了使用数字化信息的今天，以 0、1 二进制位编码在网上传递信息，连个“信封”都没有，我们发的电子邮件都是“明信片”，那还有什么秘密可言，因此，就提出了信息安全中数据的机密性需求。

数据的机密性是指数据不被未授权者获取，机密性可以保护被传输的数据免受如图 1-1 所示的截获攻击。

2. 数据的完整性

在网络环境中如何防止信息被黑客篡改，或者说信息被移花接木后怎样才可以被察觉呢？人们提出了网络中数据的完整性需求。

数据的完整性是指保证真实的数据从发送方到达接收方。在经过网络传输后的数据，必

须与传输前的内容与形式完全一样，其目的就是保证信息系统上的数据处于一种完整和未受损的状态，数据在传输的过程不会被有意或无意的事件所改变、破坏和丢失。系统需要一种方法来确认数据在此过程中没有被改变。

3. 数据的可用性

数据的可用性是授权者可以随时使用信息的服务特性，即攻击者不能占用资源而阻碍授权者的工作。由于互联网是开放性网络，需要时就可以得到所需要的数据，这是网络设计和发展的基本目标，因此数据的可用性要求系统当用户需要时能够存取所需要的数据，或者说能够得到系统提供的服务。如果一个合法用户需要得到系统或网络服务时，系统和网络不能提供正常的服务，那么就像文件资料被锁在保险柜里，开关和密码系统因混乱而不能取出一样，虽然数据完好无损地存在于系统之中，却眼看着拿不出来。例如，网络环境下拒绝服务、破坏网络和系统的正常运行等都属于对数据可用性的攻击。

4. 不可抵赖和不可否认

不可抵赖和不可否认是指用户不能抵赖自己曾做出的行为，也不能否认曾经接到对方的信息，这在网络交易系统（如电子商务）中十分重要。

另外，保护网络硬件资源不被非法占有和破坏，软件资源免受病毒的侵害，都构成了整个信息网络上的安全需求。

1.2 主要的网络安全技术

1. 密码技术

构建网络安全的体系结构离不开密码技术，没有密码技术的支撑，网络安全无从谈起。密码理论是网络安全的重要基石，是保护网络信息安全的核心与关键技术。随着通信和计算机技术发展起来的现代密码学，不仅在解决信息的机密性，而且在解决信息的完整性、可用性和抗抵赖性方面发挥着不可替代的作用。本书在第 2 章将介绍密码学中的加密技术、鉴别和数字签名等技术。

数据加密可以用来实现数据的机密性，使得加密后的数据能够保证在传输、使用和转换过程中不被第三方非法获取。数据经过加密变换后，将明文转换成密文，只有经过授权的合法用户，使用与发送方共享的密钥通过解密算法才能将密文还原成明文。反之，未经授权的用户因不掌握密钥，无法获得原文的信息。数据加密可以说是许多安全措施的基本保证。

对于数据的完整性，可以采用鉴别技术来实现，鉴别技术也是密码学的主要应用领域之一。为了防止数据在传输过程中被非法篡改、删除、产生，只需在通信介质两端进行密码学鉴别。鉴别技术就像明察秋毫的大法官，通过对鉴别算法产生的消息鉴别码的比对，立刻就能发现接收到的数据是否被做过手脚，常用的鉴别算法有消息摘要算法第五版（MD5）、安全散列算法（SHA）等。

对于通信中的抵赖行为，在密码学中可以采用“数字签名”来解决。数字签名的目的是使发送者把签了名的消息发送给接收者以后，便不能否认其签名的消息；而接收者能够验证发送者的签名，但不能伪造。数字签名的作用类似于传统的手写签名，一旦双方就消息的内容和消息的来源发生了争执，应能向仲裁者提供有效的证据，证明是一方抵赖还是另一方诬告。

2. 网络安全协议

通过前面的介绍，我们知道采用密码技术可以提供数据的机密性、完整性、抗抵赖等安全服务，那么这些安全服务如何在网络中系统地实施呢？在实际的操作中很多时候是通过网络安全协议来实现这些安全服务的。

本书在第2章中介绍的安全套接层（SSL）、IPSec就是其中有代表性的网络安全协议。虽然不必人人都是密码学或网络安全的专家，但是了解网络安全协议的基本知识无论对于计算机专业人士还是普通用户都是十分有益的，这样在具体的安全方案的实施中，可以根据实际的安全需求很方便地在操作系统和路由器中进行安全配置。

3. 身份鉴别技术

用户身份鉴别是对计算机系统中的用户进行验证的过程，让验证者相信正在与之通信的另一方就是他所声称的那个实体。用户必须提供他能够进入系统的证明，身份认证往往是许多应用系统中安全保护的第一道防线，因此，身份认证是建立网络信任体系的基础。

4. 防火墙技术

防火墙是插在内部网与外部网络之间的一个隔离层，通过建立受控的连接来形成一道安全的屏障。它隔离内部网与外部网，使内部网有选择地与外部网进行信息交换，阻止外界对内部资源的非法访问。防火墙增强了内部网络的安全性，用户可以安全地使用网络，更好地利用网络的资源。比较常用的防火墙有：包过滤防火墙、代理服务器（也叫应用级网关）、电路级网关、规则检测防火墙等。通过本章学习，我们将知道防火墙不能解决所有的安全问题，防火墙只是整个安全策略的一部分。

5. 入侵检测

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，了解网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全防线，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作等实时保护。

6. 网络病毒防护

面对病毒的猖獗，需要建立起有效的技术措施，能从病毒传染的各种可能途径入手，不受病毒种类和变形的限制，能够防、杀结合，甚至能够安全运行受病毒感染的程序，保证网络系统的有效、正常运行。

7. 数据备份与恢复

数据备份与恢复就是将系统数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。数据备份是数据可用性的最后一道防线，其目的是为了系统数据崩溃时能够快速地恢复数据，无论对于个人，还是学校、银行、证券等企事业单位，数据备份与恢复都是不可忽视的重要环节。

1.3 我国计算机网络安全现状

中国互联网络发展状况统计报告显示，截至2011年6月，中国网民规模达到4.85亿人，网民规模较2010年年底增长2770万人，迅速发展的互联网行业背后，黑色产业链的发

展也日益猖狂。统计数据显示，威胁的数量增长惊人，达到300%。与此同时，黑色链也发生了深刻的变化。

求其根源，引发网络安全问题的根源其实是“经济利益”，木马产业链、病毒经济都离不开利益。无论是盗号木马还是修改用户IE主页的恶意软件，这些病毒制作者的目的往往只有一个——“钱”。

《2010—2011中国互联网安全研究报告》显示，2010年新增计算机病毒木马1798万余种，仅从病毒数量增长情况看，病毒疫情区域平稳增长态势，感染数量没有出现类似2009年的飙升。以金山毒霸监测数据为例，2009年金山毒霸共截获新增病毒和木马20684223个，与2008年相比增长迅猛，2010年病毒数量有所下降，为17988452。图1-3为2003年到2010年的新增病毒和木马数量对比，如图1-3所示。《2011年中国互联网发展报告》显示，2011上半年，遭遇过病毒或木马攻击的网民达2.17亿，比例为44.7%；有过账号或密码被盗经历的网民达1.21亿人，占24.9%。

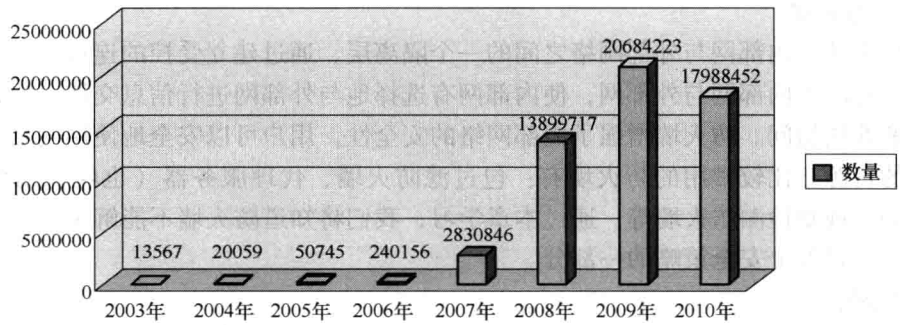


图1-3 近几年新增计算机病毒、木马数量对比

在新增病毒中，木马仍然最多，占病毒总量的73.6%。黑客后门和风险程序紧随其后，这三类病毒构成了黑色产业链的重要部分，如图1-4所示。而且网站挂马的现象也显著增

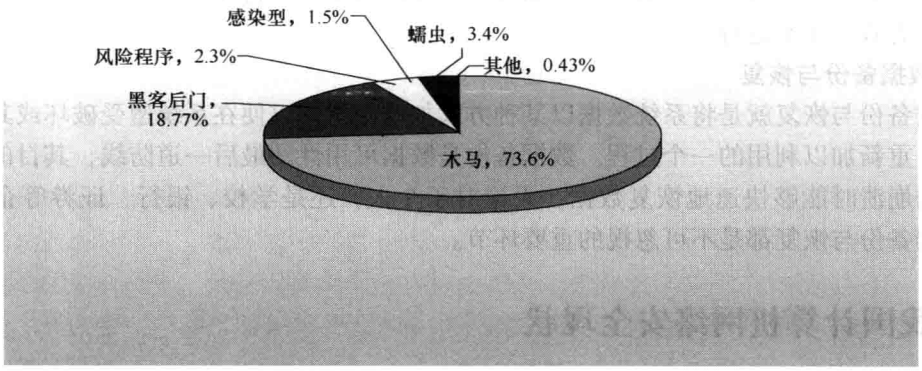


图1-4 2009年不同类别病毒和木马比例

加，网页挂马是地下产业链的重要一环，安全漏洞的披露以及网络热点事件、搜索热词的出现，都是黑客进行网页挂马的“契机”。以来自金山公司的数据显示，从2009年开始，全年共检测到8393781个挂马网站。此外，欺诈类钓鱼网站的数量也在2009年下半年迅猛增长，仅12月份，金山网盾共拦截钓鱼网站1万多个。

国家计算机网络应急技术处理协调中心（CNCERT/CC）通报的2010年网络安全数据显示，2010年一季度国家计算机网络应急技术处理协调中心共收到6225个事件报告，这个数据与2009年相比处于高位，其中垃圾邮件、网页挂马、网页仿冒事件的报告数量尤为突出，针对境内互联网基础设施的攻击主要是DoS攻击。

在公共互联网环境安全方面，国家计算机网络应急技术处理协调中心共监测发现僵尸网络控制服务器IP有3448个，僵尸网络受控主机IP有279万余个；共监测发现木马控制服务器IP有16.2万余个，木马受控主机IP有87万余个。与2009年相比，我国大陆地区的木马受控主机数量处在高位。由于目前国家计算机网络应急技术处理协调中心仅对远程控制类木马和僵尸网络进行监测，所以这些监测到的木马和僵尸网络还仅仅只能反映恶意代码活动的冰山一角。

另外，用户访问互联网的第一体验就是各种各样的Web网站，因此网站安全将严重影响用户的上网安全。2010年一季度，CNCERT共监测到我国内地被篡改网站各月累计有6488个，这一数字与2009年相比处于低位。我国被篡改网站数量的下降在一定程度上说明网站整体安全性有所提升，但总的情况不容乐观。2010年，我国内地政府网站被篡改数量各月累计达1211个；政府网站被篡改数量和比例与2009年相比处于高位。

1.4 计算机网络安全的级别分类

网络安全是建立在开放的网络环境中的，因此，建立一个严谨、统一、完整、可靠的网络信息安全标准具有非常重要的意义。

1.4.1 可信计算机系统评测标准

从1981年起，美国国防部计算机安全中心就开始全面研究计算机系统所处理的机密信息的保护要求和控制手段。1985年开发出计算机安全标准：《可信计算机系统评测标准》(Trusted Computer System Evaluation Criteria，TCSEC)，因为封面为橘色也叫橘皮书，其中的一些计算机安全级别被用来评价一个计算机系统的安全性。自从1985年它成为美国国防部的标准以来，多年来一直是评估多用户主机和操作系统的主要方法，其他子系统（如数据库和网络等）也一直是用橘皮书来解释评价的。

橘皮书就计算机系统的安全性程度，分为若干安全级别，依照安全等级由低到高的顺序是：D级安全、C级安全、B级安全、A级安全。

1. D级安全

D级是最低的安全级别，拥有这个级别的系统是可用的最低安全形式。其硬件缺乏保护，操作系统容易受到损害，用户和存储器在计算机上的信息少有身份验证控制访问权限。属于这个级别的操作系统有：MS-DOS、Windows初期版本和Macintosh System 7.x等操作系统，它们不区分用户，无法确定谁在敲击键盘，对硬盘上的信息几乎可以不受限制地访问。

它们提供简单的用户识别、验证、审核，也有一些访问控制和加密等功能，只是安全性不如C级的操作系统。

2. C级安全

C级有两个安全子级别，即C1级和C2级。

（1）C1级安全 C1级安全又称自由选择性安全保护（Discretionary Security Protection）级别，它描述了一种典型的在UNIX系统上的安全级别。这种级别的系统对硬件提供了某种程度的保护，用户拥有注册账号和口令系统，通过账号和口令来识别用户是否合法，并决定用户对程序和数据有什么样的访问权，但其硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件的访问权。文件的拥有者和超级用户（Root）可以改动文件中的访问属性，从而对不同的用户给予不同的访问权。例如，让文件拥有者具有读/写和执行的权力，而给其他用户只分配读的权力。

（2）C2级安全 C2级以C1级标准为基础，除了具有C1级包含的特性外，C2级系统还具有访问控制环境（Controlled-Access Environment）的权力。该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份认证级别。另外，系统对发生的事件加以审计（Audit），并写入日志当中，如什么时候开机，哪个用户在什么时候从哪里登录等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想强行闯入系统。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。

能够达到C2级的常见操作系统有：UNIX、XENIX、Netware 3.0、Windows NT等。

3. B级安全

B级安全也称为强制性安全保护，包括三个子级别，即B1级、B2级和B3级。

（1）B1级安全 B1级即标志安全保护（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别，这个级别说明一个处于强制性访问控制之下的对象（如磁盘或文件服务器目录），系统不允许文件的使用者修改其许可权限，这种用户标志和加密标志的双重保护，加强了系统信息的安全性。

B1级的计算机安全措施，视操作系统而定，政府机关和安全承包商们是B1级计算机系统的主要拥有者。

（2）B2级安全 B2级安全叫做结构化保护（Structured Protection），它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带及终端）分配单个或多个安全级别，它是提供较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

（3）B3级安全 B3级安全称做安全域（Security Domain）级别，使用安装硬件的办法来保护域。例如，内存管理硬件用于保护安全域免遭无授权访问或其他安全域对象的修改，该级别也要求用户的终端通过一条可信任途径连到该系统上。

4. A级安全

A级安全也称验证设计（Verify Design），是当前橘皮书中规定的最高安全级别，它包含了一个严格的设计、控制和验证过程。与前面提到的各个级别一样，该级别包含了较低级别的所有特性。其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析。可信任分布（Trusted Distribution）的含义是硬件和软件在传输过程中要受到保护，以防止破坏整个安全系统，即所有部件来源必须有安全保证，在销售和运输过程中受到严密