汪小帆　戴跃伟　茅耀斌
编　著

信息隐藏技术

●方法与应用

机械工业出版社
China Machine Press

信息隐藏技术

——方法与应用

汪小帆　戴跃伟　茅耀斌　编著

机械工业出版社

信息隐藏技术是信息安全技术研究的一个新方向。作为一本关于信息隐藏技术的专业书籍，本书系统阐述了信息隐藏技术的基本原理、具体方法及应用现状，重点介绍了数字水印技术及其在多媒体数字产品保护中的应用。

本书适合信息安全与保密通信、多媒体数字产品版权保护和电子商务安全等领域的技术人员和管理人员阅读，也可以作为通信与电子系统、信息与信号处理等专业研究生学习信息隐藏技术的入门教材。

机械工业出版社（北京市百万庄大街22号　邮政编码100037）
责任编辑：边　萌　　封面设计：姚　毅
责任印制：郭景龙
北京京丰印刷厂印刷・新华书店北京发行所发行
2001年5月第1版第1次印刷
787mm×1092mm 1/16・12印张・290千字
0 001—5000册
定价：25.00元　　（1CD，含配套书）

ISBN 7-900066-29-2/TP・27

序

20 世纪 90 年代以来，计算机网络技术和多媒体信息处理技术在全世界范围内得到了迅猛发展。一方面，网络技术的发展，尤其是 Internet 网络的大力推广，使得处在世界各地的人们进行信息交流更加方便、迅速和经济，享受到了“地球村”的乐趣；另一方面，数据压缩和多媒体技术的发展，使得人们能够方便快捷地制作、加工、分发和传送各种多媒体制品，如数字化音乐、图像、影视等方面的作品，而且这种复制和传送几乎可以无损地进行。

但是，网络在给人们带来便利的同时也暴露出越来越严重的安全问题。例如：多媒体作品的版权侵犯、软件或文档的非法拷贝、电子商务中的非法盗用和篡改、网络中信息的非法截取和查看、甚至黑客攻击等等。毫无疑问，网络中的信息安全问题是现在乃至未来相当长时期内的研究热点之一。

许多年来，各国政府和信息产业部门都很重视网络信息安全技术的研究和应用。已有的安全体制主要是建立在密码技术之上。密码技术可分为私钥和公钥两种加密体制。私钥加密体制因其密钥量大而难以实用，因此目前网络中广泛采用的是公钥加密体制。后者利用了“计算安全性”原理，一旦计算机的性能大幅度提高则会对其构成威胁。

令人惊喜的是，近年来国际信息技术研究领域出现了一个新的研究方向——信息隐藏技术研究。该技术与密码技术之不同点在于：前者隐藏信息的“内容”而后者则隐藏信息的“存在性”。该技术的出现，无疑将会给网络化多媒体信息的安全保存和传送开辟一条全新的途径。事实上，信息隐藏技术的实用化研究已在进行之中，如在 MP3 格式的音乐制品和 DVD 格式的影视作品中嵌入鲁棒水印，以进行版权保护的算法已趋成熟。

本书的作者是我系三名年轻副教授。他们在攻读博士学位期间和留校从教后的科研工作中，对信息隐藏技术、混沌控制在多媒体信息保密与隐藏技术中的应用等课题进行了较系统、深入的研究，并在中外学术期刊上发表了一系列论文。他们在书中系统介绍了信息隐藏技术的发展历史和研究现状；全面阐述了该领域中已经发展起来的一些主要技术的原理、方法和应用情况。他们本着认真负责、实事求是的科学精神，对书中给出的一些主要算法都分别编程并进行了仿真和分析。特别是对代表未来发展方向的变换域信息隐藏技术进行了深入的探讨并给出了最新的研究成果。

据我所知，目前国内尚未见到系统地介绍信息隐藏技术方面的专著。因此，本书的出版，对信息隐藏理论与技术的传播与应用是适时的，是符合广大读者需要的，将会对我国信息隐藏技术的研究发展和应用做出应有的贡献。

南京理工大学自动化系　　王执铨（教授）

前　言

你也许知道间谍用隐形墨水技术传递秘密信息的方法，但你知道如何在 Internet 上把秘密信息隐藏起来进行传递吗？你肯定知道人民币上的水印是鉴别真伪、防止盗版的重要标志，但你了解如何在各种数字化产品(如电子图书、数字图像、音乐、视频等产品和数量巨大的网页内容等)中加入数字水印以有效地保护版权吗？这些问题正是本书介绍的信息隐藏技术的两个主要分支——隐秘术和数字水印技术的研究内容。

公钥密码体制的发明人之一 Rivest 曾说过："需要是发明的母亲，而计算机网络就是现代密码学的母亲"。20 世纪 70 年代计算机网络的兴起正是掀起现代密码学研究热潮的主要推动力，并使之发展成为一门相对成熟的学科。随着 20 世纪 90 年代 Internet 的迅速发展，多媒体技术的逐渐成熟和电子商务的兴起，网上多媒体信息量急剧膨胀。一方面，这使得把秘密信息隐藏在普通多媒体信息中传输成为可能，并需要有把这种可能变为现实的技术；另一方面，这也迫切需要有保护各种数字产品的有效手段。这两方面的需求正是多媒体信息隐藏技术研究的推动力。因此，我们可以说"计算机网络是现代密码学的母亲，而 Internet 就是现代信息隐藏技术的母亲"。

自从 1996 年召开第一届关于信息隐藏技术的国际会议以来，信息隐藏技术的理论、方法及应用研究正越来越广泛地受到关注，一些公司已开始推出相应的产品。可以预见，随着网络信息时代的发展，信息隐藏技术的研究也会逐渐走向成熟。目前有关信息隐藏的文献众多且分散，国际上虽然出版了一本关于信息隐藏技术的英文书籍，但该书是由一些综述性文章合编而成的，对已有一定研究基础的专业研究人员较为合适，却不适合初学者阅读。我们编写本书的目的就是希望系统介绍信息隐藏技术的基本原理、具体方法及应用现状，以使我国能有更多的人了解、使用和研究信息隐藏技术，满足国内从事信息隐藏技术研究、开发及应用的有关人员的需要，为推动我国信息安全技术的发展尽一份力。

本书共分 7 章。由于信息隐藏技术是信息安全技术的一个新的研究分支，我们在第 1 章简要介绍了网络信息安全技术。信息隐藏技术与信息加密技术有着密切的联系，信息隐藏与信息加密都是把对信息的保护转化为对密钥的保护，因此信息隐藏技术沿袭了传统加密技术的一些基本思想和概念。严格说来，密码学是一门涉及许多复杂数学理论的学科，我们在第 2 章中力求用浅显的语言向广大读者介绍密码学的基础知识。第 3 章综述了信息隐藏技术的基本概念与原理、应用领域和发展概况。第 4 章叙述了隐秘术的基本原理与方法，并分析了一些常用的隐秘软件。第 5 章~第 7 章介绍的数字水印技术是目前信息隐藏技术研究的重点，我们详细阐述了图像水印技术、语音水印技术和视频水印技术，并介绍了水印系统的性能分析和测试手段，分析了常用的数字水印软件。本书所附光盘包括多种信息隐藏及水印技术的共享软件、免费软件、测试图库、相关链接、开发工具等。

本书由南京理工大学自动化系的汪小帆、戴跃伟和茅耀斌三位教师编著，但本书得以在较短时间内完成是与很多人的支持分不开的。我们首先要特别感谢王执铨教授对本书的审阅及提出的建设性意见。近几年来，王执铨教授一直努力为我们创造和谐的科研环境，并对我们的科研工作始终给予了有力的支持和指导。孙金生副教授参与了本书内容的讨论，

硕士研究生杨洋和朱晓松分别参与了语音水印技术和小波域图像水印技术相关内容整理和算法仿真，硕士研究生杨凯丰在本书附带光盘的制作中提供了帮助，硕士研究生卓成春参与了相关仿真程序的编制和调试，在此一并致谢。

虽然信息隐藏技术作为一门极有市场前景和挑战性的新兴学科，已引起了大批科研工作者的研究兴趣。但毕竟发展时间很短，理论基础还不完善，实用化技术还欠成熟。因此更需要我们共同努力来进行研究和促进发展。

由于水平有限，且时间仓促，书中缺点和不足在所难免，敬请广大读者批评指正。同时作为具有控制科学与工程专业背景的研究人员，我们深知反馈的重要性。因此，我们热忱希望读者能把对本书的任何意见及时反馈给我们。

编 著 者

目　录

第 1 章　网络信息安全概论

1.1 网络时代的到来

Intel 三巨头之一的摩尔(Gordan Moore)在 1965 年提出了著名的“摩尔定律”，指出 CPU 的晶体管数目和性能大约每 18 个月增长一倍，该预言已为过去几十年 CPU 的发展历史所证实。个人电脑中 CPU 的晶体管数目从最初的两千多个发展到了以千万计，而 CPU 速度则已达到了 1G 数量级。早些年前就有人担心摩尔定律的物理极限要到了，但至少在近期还看不出速度减慢的势头，而且一种技术的尽头也许正是另一项新技术的开始。不仅如此，存储技术，带宽技术及其他一些通信技术的发展速度比摩尔定律确定的速度还要快！如在过去 10 年中，光纤的传输能力每 6 个月就翻一番，这被称为光纤传输定律，其速度比摩尔定律描述的速度快了 8 倍。可以预见，几年以后，用几千元人民币就可买到一台拥有 2000MHzCPU、1GB 内存和 50GB 硬盘的计算机。这台计算机，在公司可接上千兆以太网或十兆无线网络，在家中可用 1Mbps 以上速度的电话或电视网络上网。许多今天的梦想都会成为现实，让你真正体验到“精彩世界，瞬间拥有”。

随着计算机和网络技术的快速发展，在过去几年中，Internet 的规模也急剧膨胀。以中国为例，Internet 上网用户 1997 底为 62 万户，1998 年底为 210 万户，到 1999 年底发展到 890 万户，平均也是每 6 个月翻一番！我们有理由相信，在不久的将来，不但电脑和手机可以上网，而且各种家用电器、汽车、控制设备等都可以连接到网上。当然，Internet 的意义并不在于网络本身，而在于它给人类社会带来的深刻变化。以太网技术发明人，被誉为 IT 界的“格林斯潘”的梅特卡夫(Bob Metcalfe)早就预言 Internet 的影响将以几何级数增长，这被称为“梅特卡夫定律”。确实，随着以 Internet 技术为代表的信息技术的飞速发展，人类社会正在经历巨大的变革，人们的生产方式、生活方式、意识形态、思维方式都因网络的冲击、信息化的推进而发生着巨大的变化。

以一句“网络就是计算机”震撼 IT 产业的 Sun 公司还有一句著名的广告词：“人类文明从网络开始”。其实，我们早已生活在各种各样的网中，从电力网、电话网、广播电视网、商业网到公路网、铁路网、航空网等交通网。但却没有任何一个网如 Internet 一样，在如此短的时间内影响如此多的人。在普通场合，网络已成为 Internet 的代名词。Internet 打破了传统的边界概念，使世界变得越来越小，而市场变得越来越大，广阔的世界宛如地球村，远隔万水千山的贸易伙伴如同就在眼前。随着以 Internet 为代表的网络信息技术的继续发展，全球经济一体化和信息网络化相互依存、相互促进的趋势越来越明显，并将成为我们这个地球上所有公民的共同目标。事实上，在一些高科技发达的地区(如美国的硅谷)，人的衣、食、住、行都已经离不开 Internet。出门先要上网打出一个路线图，买东西要先到网上转一圈，订房间、买

机票更是要靠上网解决。置身于这个把网络融入日常生活的环境中，你还会认为网络经济完全是泡沫吗？

在网络信息时代，“任何的产品、技术都要考虑到互联网，错过一段时间可以原谅，但最可怕的是错过一个时代”。电子商务作为网络时代经济活动全新的技术手段和方法，已成为 Internet 最广阔的应用领域。电子商务是指在网络环境特别是 Internet 上所进行的商务活动。从交易的参与者来看，电子商务有企业对企业（B to B），企业对消费者（B to C）和消费者对消费者（C to C）等几种类型。目前的电子商务活动包括三个方面的内容，一是网上信息服务，如在网上发布广告和商情，进行产品宣传和客户问题解答，使用维护指导等。二是电子购物与贸易，进行询价、报价、订单、签约、电子支付和商品交付。三是电子银行与金融服务，在网上开设银行与保险业务，为企业商务活动和个人理财提供金融和保险服务。许多国家政府和世界性组织在近几年先后制定了发展电子商务的相关政策。例如，联合国国际贸易法委员会于 1996 年 6 月提出了电子商务示范蓝本，1997 年 4 月，欧盟提出了“欧盟电子商务行动方案”，1997 年 7 月，美国政府发表了“全球电子商务框架”文件，1998 年 9 月，新加坡政府宣布了“新加坡电子商务发展计划”。IT 业的各大著名公司，如 IBM、Microsoft、Intel、Compaq、HP、Cisco、Sybase、SUN 和联想等，纷纷提出了电子商务策略。尽管在电子商务的发展过程中尚存在许多问题和“泡沫”，但作为未来经济的发展方向，其前景无疑是十分广阔的。在网络经济时代，各国政府也都面临着角色转换，适应时代要求的新课题，尤其是政府部门在协助本国国民和各行业把握互联网经济的潜能方面，发挥着越来越重要的作用。许多国家都先后提出了构建电子政府的纲领。我国也于 1999 年启动了“政府上网工程”。

人类正站在世纪之交的门坎上，迎接着网络时代与信息社会的到来。美好的未来值得人们去憧憬，美好的未来也预示着新的问题与挑战。

1.2 网络信息安全的威胁

网络上流动的是信息，信息是网络时代最重要的资源。随着以 Internet 为标志的网络时代的到来和以电子商务为代表的网络经济的兴起，网络信息安全问题也日益突出。网络是一柄双刃剑，人们在享受网络带来的便捷与高效的同时，也面对着同样“便捷”与“高效”的网上作案手段。从个人事务、企业商务到政府运作，网络信息安全已成为最令人感到不安和担忧的因素之一。如何保护政府、企业和个人的信息不被非法获取、盗用、篡改和破坏，已成为所有 Internet 参与者共同关心的重要问题。从网络安全立法到安全技术的实施，人们在追随技术发展的同时不懈地寻找问题的解决方案。在安全性未得到有效保证之前，电子商务和电子政府等模式将无法发展到应有的层次和深度。网络信息安全已成为影响国家安全、经济发展、个人利益和社会稳定的重大关键问题。从保护国家和个人的利益出发，各国政府无不重视信息和网络安全。特别是各发达国家均大力加强信息安全的研究和督导。美国将推出面向 21 世纪的新的数据加密标准方案，并制定了更加严格的信息安全产品出口政策。同时，各大跨国公司如 IBM、HP、SUN 等均建有强大的信息安全实验室。从我们国家的安全和民族

利益出发，网络信息安全问题不研究不行，仅仅满足于分散的、以封堵已发现的安全漏洞为目的的研究也不行。而必须从基础着手，对网络环境下的信息安全开展强力度的研究，为我国的信息安全提供崭新的、整体的理论指导和基础构件的支撑，并为信息安全技术的实现奠定坚实的基础。

网络与安全本身就是一对矛盾，任何时候都不可能有绝对的网络安全。依据 Financial Times 曾做过的统计，平均每 20s 就有一个网络遭到入侵。但同时，安全又是电子商务发展的根本，企业与消费者对电子交易安全的担忧严重阻碍了电子商务的发展。如何改进电子商务的现状，让用户不必为安全担心，是推动安全技术不断发展的动力。另一方面，互联网应用不仅仅是网上购物、网上拍卖、网上服务等，还应包括电子政务，如电子邮件、网上信息发布、在线办公等。信息安全产业固有的敏感性及特殊性，直接影响着国家的安全利益和经济利益，所以国家对信息安全产品的研制、生产、销售，使用及进出口要实行严格及有效的管理控制。所有这些因素都呼唤国内的信息安全产业早日发展并成熟起来。

安全性问题也是构建“电子政府”面临的严峻挑战。由于政府形象及保密因素，“电子政府”工程对安全性提出较高要求。而在目前技术条件下，安全性成为热衷构建“电子政府”的各国共同面临的一大难题。为此，日本政府已决定在 2000 年拨款 24 亿日元，加紧研究开发提高计算机系统保密和安全性能的技术，其中包括检测和消除计算机病毒的技术以及数据加密技术等。

下面我们简单介绍一下对网络信息安全的几个主要威胁。

1.2.1 黑客攻击

“黑云笼罩网络世界，网络黑客惊扰全球”，这是一篇有关黑客的新闻报道的标题。现在人们几乎每天都能看到有关黑客的报道。20 世纪 60 年代早期，拥有巨型计算机的大学电脑设施——如麻省理工学院的人工智能实验室成为黑客初显身手的舞台。最初，“黑客”（hacker）是一个褒义词，指的是那些尽力挖掘计算机程序的最大潜力的电脑精英。但目前黑客的普遍含义是指计算机网络系统的非法入侵者。人们一直认为电脑黑客大都是计算机方面的天才。他们中的许多人只有十几岁，或是刚二十出头，但已开始使用高新技术去闯入或攻破他人的计算机系统。他们常自称为信息时代的侠盗罗宾汉，通过寻找出计算机系统的漏洞，他们可以使跨国公司和政府机构的网站崩溃，甚至于一些专门从事网络安全技术的公司的网站也未能幸免于难。

1998 年，美国国防部宣布黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，打入了许多政府非保密性的敏感电脑网络，查询并修改了工资报表和人员数据。不久，警方抓获了两名加州少年黑客。三个星期后，美国警方宣布以色列少年黑客“分析家”被抓获。1999 年 5 月～6 月，美国参议院、白宫和美国陆军网络以及数十个政府网站都被黑客攻陷。

1999 年 11 月，挪威黑客组织“反编译工程大师”破解了 DVD 版权保护的解码密钥。该组织编制了一个 DVD 解码程序公布在互联网上，这个举动引发了一系列诉讼

案。一名黑客在勒索一家网上音乐 CD 零售公司未达到目的的情况下，便把偷来的该公司信用卡密码复制了成 千上万份在网上公布。

2000 年 2 月，在三天的时间里，黑客使美国数家顶级互联网站，如 Yahoo!、Amazon、eBAY、CNN 等陷入瘫痪。与黑客侵入美国国防部、美国海军研究实验室、国家宇航局及洛斯阿拉莫斯国家实验室的计算机网络事件不同的是，此番黑客袭击的目标转移到了如日中天的著名商业网站，而且，袭击的目的只有一个：造成网络瘫痪。显然，以网络瘫痪为目标的袭击效果比任何传统的恐怖主义和战争方式都来得更强烈，破坏性更大，造成危害的速度更快，范围也更广。而袭击者本身的风险却非常小，甚至可以在袭击开始前就已经消失得无影无踪，使对方没有实行报复打击的可能。据报道，此番商业网站遭难的技术原因，从手法上分析极为简单。黑客使用了一种称作“拒绝服务式”的攻击手段，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。为应付急速增长的数据量和访问量，各大网站的服务器容量也越来越大，一些网站巨头的数据量已经达到了 TB 级(TeraByte，即 2 的 40 次方个字节，大约相当于 73 万张 1.44MB 的软盘)。不过，无论数据量有多大，黑客此番攻击的逻辑却非常简单，只要用大量毫无意义的数据垃圾，快速而又反复地挤占路由器，让数据通道为这些无法识别其真实目的数据“忙个不休”。如此简单的思路和手法，却十分有效。这充分说明了网络安全问题的紧迫性和严重性。

2000 年 6 月 16 日晚，全世界最大的网站“美国在线”遭到黑客攻击，其中一名黑客透露了他攻击美国在线时采用的主要技术手段。据称，美国在线的安全缺陷就在于其客户关系信息系统(CRIS)，该系统是与美国在线用以保存 2300 万客户帐户、信息以及其他资料的主要数据库相联的用户界面。这次美国在线遭到攻击，就有几百个帐户的资料被窃取，其中包括客户的姓名、住址、电话以及信用卡等资料。

我国的形势也不容乐观。据报道，目前国内电子商务站点中，90%以上存在严重的安全漏洞。统计表明，近年来利用网络进行的各类违法行为在中国以每年 30%的速度递增，目前已发现的黑客攻击案约占总数的 15%，多数案件由于没有造成严重危害或商家不愿透露而未被曝光。据媒介报道，中国 95%上网的网管中心都遭到过境内外黑客的攻击或侵入，其中银行、金融和证券机构是黑客攻击的重点。据新浪网透露，2000 年 2 月 8 日下午，电子邮件系统突然冲进数以百万计的电子邮件，系统堵塞、崩溃达 18 小时。

使人们害怕的是，不仅仅是黑客攻击造成的后果，而且还有它所蕴含的潜在威胁。全球网络化已是一个不可逆转的趋势，网络在人们生活中的作用将越来越大。人们不难想像黑客攻击一旦得逞，小则网络某项服务瘫痪，大则造成一定时间内整个网络的堵塞，导致无法估量的损失。尽快遏制黑客的嚣张气焰，保护互联网的健康发展，已成为各国的当务之急。有鉴于此，一些国家纷纷制定有关措施和法律，打击网络犯罪，切实维护网络安全。此外，黑客犯罪是一种技术犯罪，要有足够的技术手段才能防范制止，相应的技术保障必不可少。值得注意的是，由于一些国家对信息安全技术出口的限制，建立在别人技术之上的安全是不可靠的，我国必须下大力气研制自主版权的网络信息安全技术。

1.2.2 计算机病毒

随着计算机的不断普及和网络的迅猛发展，计算机病毒造成的危害也越来越大。1999 年 4 月 26 日的 CIH 病毒大爆发给我国带来了数以亿元计的损失。2000 年 5 月 4 日，看似浪漫多情其实奇毒无比的“I love you”病毒肆虐 Internet，并在 2 个小时以内，就造成了 10 多亿美元的损失。这种病毒隐藏于一封署名“I love you”的电子邮件中，一旦被阅读者打开，阅读者的电子邮件档案便遭到侵入，里面所有的地址都会再收到这封邮件，从而造成全球各地多起电脑网络系统发生严重“当机”事件。由于这种病毒会窃取有关个人身份信息和密码，也引发了人们对密码安全的关注。普通密码通常只是具备单一信息的固定认证方式，这类密码极易被窃取或更改，因而难以提供足够的安全保障。用户为使用方便，往往在选取密码后，便直接将其储存于系统内。目前许多组织和机构已纷纷采用了保密性更强的双重密码验证系统，用户只有提供两种以上的身份验证内容，才能存取特定的信息资源。例如，ATM 自动提款机要求用户提供 ATM 提款卡和个人密码两种形式的身份验证，窃取者如欲擅入帐户，则必须同时获取这两种密码，从而大大降低了密码被窃取的风险度。

在《中华人民共和国计算机信息系统安全保护条例》中指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。计算机病毒程序的基本特征包括：

传染性　它们会在使用者尚不察觉的情况下将自身复制并传染给正常的计算机文件。

隐蔽性　一般正常程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户来说是可见的、透明的。而病毒程序的执行是在用户不知的情况下完成的，它的动作、目的对用户来说是未知的。

破坏性　计算机病毒的种类很多，其破坏性的表现方式也很多，我们可以大致按照破坏方式和破坏力的大小将病毒分为良性病毒、恶性病毒、极恶性病毒和毁灭性病毒。良性病毒的发作表现往往是显示信息、奏乐、发出声响。恶性病毒则会干扰计算机运行，使系统变慢、死机、无法打印等。极恶性病毒会导致系统崩溃、无法启动，其采用手段通常是删除系统文件、破坏系统配置等。毁灭性病毒对于用户来说是最可怕的，它通过破坏硬盘分区表、 FAT 区、引导记录、删除数据文件等行为使用户的数据受损失，如果没有做好备份，则损失将无法挽回。

早期计算机病毒主要是靠拷贝软盘上的软件进行传播的，尤其是引导型病毒，但自从有了计算机网络，病毒就通过网络迅速传播。在网络环境下，网络病毒除了具有可传播性、可执行性、破坏性、可触发性等计算机病毒的共性外，还具有一些新的特点：

感染速度快　在单机环境下，病毒只能通过软盘从一台计算机带到另一台，而在网络中则可以通过网络通信机制进行迅速扩散。

扩散面广　由于病毒在网络中扩散非常快，扩散范围很大，不但能迅速传染局域网内所有计算机，还能通过 Internet 将病毒在一瞬间传播到千里之外。

传播形式复杂多样 计算机病毒在网络上一般是通过“工作站－服务器－工作站”的途径进行传播的，但传播的形式复杂多样。

难于彻底清除 单机上的计算机病毒有时可通过删除带毒文件，低级格式化硬盘等措施将病毒彻底清除，而网络中只要有一台工作站未能消毒干净就可使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台工作站就有可能被网上另一台带病毒工作站所感染。因此，仅对工作站进行病毒杀除，并不能解决病毒对网络的危害。

破坏性大 网络上病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络崩溃，破坏服务器信息，使多年工作毁于一旦。

目前各种新的病毒仍以长江后浪推前浪之势不断涌现，对网络信息安全造成很大的威胁。但我们也不必要谈“毒”色变，只要了解病毒的本质、熟悉病毒传染破坏规律并有防患于未然的意识，是可以建立起坚固的防毒堡垒的。

1.2.3 侵犯个人隐私与版权

在科幻片《网络惊魂》中，女主角平日离群索居，只通过网络与外界打交道。在网上洽谈和处理公务、购物、娱乐等。但有一天，她突然被卷入了一起谋杀案，才发现自己在网上的一举一动都被监视着，个人信息资料也被篡改，使她从一个安分守己的弱女子变为一个前科累累的通缉犯。今天看来，这已不再是科幻，而完全有可能成为现实。

当个人在网上浏览、咨询或购物时，往往要填写一些个人信息，如姓名、生日、性别、信用卡号、家庭地址、电话号码、E-mail 地址、个人爱好和工作性质等。这就涉及到如何有效地保护个人隐私的问题。商家可能会把收集到的个人资料存放在专门的数据库中，然后经过数据加工和处理得到有商业价值的信息。从商家角度看，其目的可能是为了向消费者提供更优质的服务；而从消费者角度看，有些人就会感到个人隐私受到侵犯。此外，网上还有一些公司通过各种渠道收集大量个人资料，然后未经个人同意就明码标价公开出售，这更是完全侵犯了个人隐私。为此，一些国家和地区制订了保护个人隐私的政策和措施，如香港特区政府设立了专门的私隐专员并在《香港个人资料（私隐）条例》中对企业作了如下规定：

“应为浏览网页者及消费者提供使用匿名身份的选择；应制定个人资料私隐政策：包括收集个人资料的目的，使用资料及披露资料的方式，提供“拒绝服务”的选择，查阅及改正资料的程序，投诉及纠正机制以及在有关情况下制定向儿童收集个人资料时须先取得家人同意及受家人管制的政策；应在本企业网址上展示上述政策；在收集敏感性资料时采取加密措施。”

网络信息时代的到来也对版权保护提出了新的挑战。所谓版权，有时也称作者权，在我国被称为著作权，是基于特定作品的精神权利以及全面支配该作品并享受其利益的经济权利的合称。随着网络规模的不断扩大和数字化技术的不断成熟，网上各种数字化图书、报刊杂志、绘画、照片、音乐、歌曲及影视作品的数量也急剧增加。这些数字化产品和服务都可实现网络传送，不受时间空间限制，甚至无须物流运输，在交易和支付完成后，就可高效快捷地通过网络提供给客户。而网络的开放性和资源

共享使得如何有效地保护网络数字化产品的版权成为一个十分重要的问题。必须有行之有效的技术手段以防止对网络数字化产品的篡改、假冒、剽窃和盗用等。

“需要是发明的母亲”，多媒体数字产品的版权保护正是近几年兴起的数字水印技术的主要推动力，本书将对数字水印技术的研究现状作系统介绍。

1.3 网络信息安全技术概述

“网络改变世界，安全改变网络”。以电子商务为例，假设您作为交易人，无论您从事何种形式的电子商务都必须清楚以下事实：您的交易方是谁？信息是否可靠？这些信息（如个人资料和数字产品）通过网络传递是否安全？交易的合法性如何？等等。因此，企业与消费者对电子交易安全的担忧是必然的，如何改进电子商务的现状，让用户不必为安全担心，是推动安全技术不断发展的动力。

网络信息安全涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计三方面，当然也包括对用户的鉴别和授权。为保障数据传输的安全，需采用数据传输加密技术、数据完整性鉴别技术；为保证信息存储的安全，须保障数据库安全和终端安全；信息内容审计，则是实时对进出内部网络的信息进行内容审计，以防止或追查可能的泄密行为。对用户的鉴别是对网络中的主体进行验证的过程，通常有三种方法验证主体身份。一是只有该主体了解的秘密，如口令、密钥；二是主体携带的物品，如智能卡和令牌卡；三是只有该主体具有的独一无二的特征或能力，如指纹、声音、视网膜或签字等。

网络信息安全的技术特征主要表现在以下几个方面：

完整性(Integrity)——是网络信息未经授权不能改变的特性。即对抗主动攻击，保证数据的一致性，防止数据被非法用户修改和破坏。

保密性(Confidentiality)——是网络信息不被泄露给未经授权者的特性。即对抗被动攻击，以保证机密信息不会泄露给非法用户。

可用性(Availability)——是网络信息可被授权者访问并按需求使用的特性。即保证合法用户对信息和资源的使用不会被不合理地拒绝。

不可否认性(Non-repudiation)——也称为不可抵赖性，即网络上所有参与者都不可能否认或抵赖曾经完成的操作和承诺。发送方不能否认已发送的信息，接收方也不能否认已收到的信息。

可控性(Controllability)——是对网络信息的传播及内容具有控制能力的特性。即能够对网络信息实施安全监控。

保护信息安全所采用的手段也称作安全机制。所有的安全机制都是针对某些安全攻击威胁而设计的，可以按不同的方式单独或组合使用。合理地使用安全机制会在有限的投入下最大地降低安全风险。网络中所采用的安全机制主要有：

信息加密和隐藏机制——加密使有用的信息变为看上去无用的乱码，攻击者无法读懂信息的内容从而保护信息；而隐藏则是将有用的信息隐藏在其他信息中，使攻击者无法发现，不仅实现了信息的保密，也保护了通信本身。至今，信息加密仍是保障信息安全的最基本的手段。信息隐藏是信息安全领域的一个新方向，它在数字化产品

的版权保护等领域的应用中正越来越受到人们的重视，本书的目的就是对信息隐藏技术作全面而系统的介绍。

完整性保护——用于防止非法篡改，利用密码理论的完整性保护能够很好地对付非法篡改。完整性的另一用途是提供不可抵赖服务，当信息源的完整性可以被验证却无法模仿时，收到信息的一方可以认定信息的发送者，数字签名就可以提供这种手段。

认证机制——网络安全的基本机制，网络设备之间应互相认证对方身份，以保证赋予正确的操作权力和数据的存取控制。网络也必须认证用户的身份，以保证合法的用户进行正确的操作并进行正确的审计。

审计——防止内部犯罪和事故后调查取证的基础，通过对一些重要的事件进行记录，从而在系统发现错误或受到攻击时能定位错误和找到攻击成功的原因。审计信息应具有防止非法删除和修改的措施。

权力控制和存取控制——主机系统必备的安全手段，系统根据正确的认证，赋予某用户适当的操作权力，使其不能进行越权的操作。该机制一般采用角色管理办法，针对系统需要定义各种角色，如经理、会计等，然后对他们赋予不同的执行权利。

业务填充——在业务闲时发送无用的随机数据，增加攻击者通过通信流量获得信息的困难。同时，也增加了密码通信的破译难度。发送的随机数据应具有良好的模拟性能，能够以假乱真。

第 2 章　密码技术简介

2.1 基本概念

密码学（Cryptography）是把有意义的信息编码为伪随机性的乱码以保护信息的一门学科。而研究如何破译密码的学问称为密码分析学（Cryptanalysis）。密码学和密码分析学是保密学（Cryptology）的两个相互对立又相互促进的分支。

尽管保密学是一门涉及到许多艰深数学理论的学科，但普通网络用户还是能够，而且应该了解其基本概念和思想的，这也正是本章的目的之一。通常把待加密的消息称为明文（Plaintext），加密后的消息称为密文（Ciphertext）。加密（Encryption）就是从明文得到密文的过程；而合法地由密文恢复出明文的过程称为解密（Decryption）。加密和解密所采用的规则分别称为加密算法（Encryption Algorithm）和解密算法（Decryption Algorithm）。加密算法和解密算法统称密码算法。密码算法是在一组称为密钥(Key)的参数的控制下进行的。

在密码学研究中，人们习惯上根据英语的首两个字母 A 和 B，把通信的双方分别称为 Alice 和 Bob。根据 Eavesdropper（偷听者）的第一个字母 E，把企图偷听 Alice 和 Bob 之间的通信的人称为 Eve。也称 Eve 为被动攻击者。根据 Malicious（怀恶意的）的第一个字母 M，把可能篡改和伪造消息的恶意窃听者称为 Mallet。也称 Mallet 为主动攻击者。被动攻击的隐蔽性强，而主动攻击的破坏性大。图 2-1 是密码通信系统结构示意图。

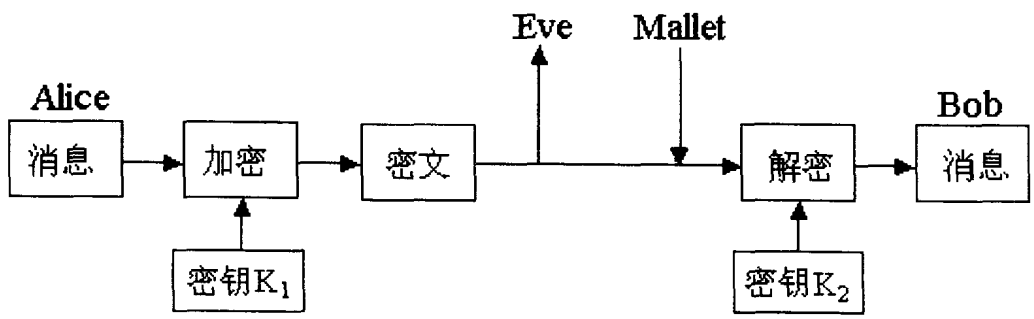

图 2-1 密码通信系统模型

在密码学中，有一个基本的 Kerckhoffs 假设，即秘密必须全寓于密钥中，而密码算法可以且应该公开。密码学的历史表明，企图靠掩盖密码算法以保护信息的方法往往是失败的。

常用的密码分析攻击包括以下几类：

（1）唯密文攻击（Ciphertext Only Attacks）　分析者只知道截获的密文。

（2）已知明文攻击（Know-Plaintext Attack）　分析者不但能截获密文，而且能得到一些明文—密文对。