21世纪网络工程丛书——安全防卫系列

附CD

黑客攻击技术揭秘

许榕生　刘宝旭　杨泽明　等编著

机械工业出版社
China Machine Press

21世纪网络工程丛书——安全防卫系列

黑客攻击技术揭秘

许榕生　刘宝旭　杨泽明　等编著

机械工业出版社

本书在回顾网络信息安全发展的基础上，总结了网络信息安全的特征，介绍了网络信息安全要素的分类与常见的网络攻击行为，对危害网络信息安全的黑客攻击技术进行了深入细致的分析讲解，使大家对黑客的攻击手法有一定的认识与辨别能力。全书共分12章，包括：网络信息安全的发展与特征、网络运行平台安全因素、信息内容安全、文化安全、黑客、入侵系统类攻击、欺骗类攻击、拒绝服务攻击、攻击防火墙、病毒攻击、木马程序攻击及信息战。

本书适用于关心我国网络信息安全发展的各界人士，特别对广泛应用网络进行工作与交流的人员有很好的参考价值。针对本书的读者对象，书中讲述力求深入浅出，通俗易懂，注重科学性与实用性，并配有精选实例，供读者参考。

本书对网络信息安全领域的专业技术人员及信息时代的创业者都不失为一本实用的工具书，同时每一个人都可以分享他人的经验，使本书发挥更大的作用。

图书在版编目（CIP）数据

黑客攻击技术揭秘/许榕生等编著. —北京：
机械工业出版社，2002.4
（21世纪网络工程丛书——安全防卫系列）
ISBN 7-111-09886-2

Ⅰ.黑… Ⅱ.许… Ⅲ.计算机网络-安全技术
Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2002）第006997号

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　汪汉友
责任印制：路　琳
北京机工印刷厂印刷·新华书店北京发行所发行
2002年4月第1版第1次印刷
1000mm×1400mmB5·8.25印张·320千字
0001-5000册
定价：29.00元(含1CD)
凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、68326677-2527

序　言

国庆与中秋双节前夕，作者将其姊妹篇《黑客防范技术揭秘》和《黑客攻击技术揭秘》书稿交给了我，委托我为这两本新作做序。月圆长假,我本想处理些其他任务的我，只好遵托响应了这个优先中断。端坐屏前逐章拜读。书中的描述和现实的世界不时显现心头。

攻与防，自古为兵家研习的方略，信息化发展的今天却依然困扰着原本欣喜的世人。信息革命带给人们的遐想，像一轮中天的明月如歌如赋。但“9·11”纽约世贸双子星在暴力和恐怖面前的消失，使人们从遐想中清醒。“世界未到大同时，太平难自空中降”，我们必须为信息革命付出代价，认真对付阻碍信息化健康发展的“无知”、“恐怖”与“暴力”。

为什么像书中提到的那样，我们的信息系统存在那么多的漏洞？看来本质上还是我们的“无知”。人类认识真理和正确地进行社会实践的过程是一个求极限的趋近过程。在这个规律的“惩罚”下，再能干的人所编写的程序，设计的电路，依然免不了存在错误。记得在一次国际会议上 IBM 的一位专家说，平均 1000 行源程序中就可能存在 1 处错误（Bug），而在这个国际会议的另一次年会上，应用密码学的作者布鲁斯·斯奈尔认为比这还要多，平均达到 5~50 个之多。今天操作系统和应用程序的规模动辄上百万行，上千万行。出错的可能性实在太大了，难怪我们用计算机时常莫名其妙地“死掉”。

无知不仅仅伴随着设计和制造者，它更是使用者的隐患。初为电子公民，对许多知识、技能、道德、规则了解不多或没认真遵循，不仅常会坑害自己，还会殃及他人。

除了以上内因，造成信息安全事件层出不穷的外因是世界上存在着犯罪、竞争、斗争和战争。这些因素驱使一些人和组织，甚至国家花费大力发掘信息系统客观存在的漏洞，使劲儿设法钻进未被授权的系统去窥视他人，欺骗、偷窃、破坏和制造信息世界的恐怖和暴力。他们不但利用系统的漏洞，还会有意放置一些后门和木马，以便长期控制他人，达到利己的目的。

人类追求的真善美，伴随了这些不协调的假、恶、丑，使数字化的信息空间如被乌云遮盖的一轮明月。

为了和这些假、恶、丑斗争，必须加强对信息安全保障的研究。这几年来，国内翻译、编辑出版了不少有关信息安全的书籍。也出现了一批我国科学技术工作者自己撰写的书籍。这个姊妹篇就是这批书籍中的两本。两本书从攻和防两个角度介绍论述了同一个问题的两个侧面，使人们读起来更有味道。这套书的特点是不但论述了技术而且论述了管理，不但论述了原则，而且论述了实践

技巧，同时还给出了许多实例，从宏观和微观两个方面给人以启示。其中不乏作者们自己的亲身实践经验与体会，确可使人开篇有益。

愿更多的人们投身于对假、恶、丑的斗争，愿信息化社会的发展持续健康，让我们用自己的双手送别明月，迎接信息革命成功的一轮朝阳。

中国科学院研究生院
信息安全国家重点实验室
赵战生

2001 年国庆节于北京

前　言

目前国内业界人士已普遍达成共识：我们的世界正在演变为一个电子化的世界（E-World），所有的信息正在全面数字化，电子世界中四通八达的网络把人们联系在一起。在网络上，天涯变为咫尺，物理上的距离几乎都消弭于无形，人们可以运筹帷幄，决胜于千里之外。统计显示，因特网发展的速度超过了以往所有其他技术。无线电广播问世 38 年后拥有 5000 万听众，电视诞生 13 年后拥有同样数量的观众，而因特网从 1993 年对公众开放到拥有 5000 万用户只花了 4 年时间。目前，全世界因特网使用者超过 2 亿，到 2001 年底因特网使用者已达 10 亿。然而，伴随着网络的迅猛发展，一系列问题也随之而来：如何建设和发展网络？在我国有没有条件推广使用？其制约因素是什么？……

我国的信息化进程，经历了单机、专用局域网、广域网到 Internet 的发展阶段。“三金”系列工程中，许多工程都利用物理的公用网络条件来实施逻辑的专业和行业应用，因此说，以 Internet 为代表的信息网络正在成为未来全球信息系统的最重要的基础设施。这一发展变化使我们的信息安全观念必须有所拓展。

网络由智能设备构成，而智能设备将按照制造者或设计者的意图执行使用者或拥有者的指令。当制造者与拥有者的利益发生冲突时，智能设备会站在哪一边是由制造者在制造时确定的。不能保证制造者的意图全部向使用者或拥有者公开，这包括个别设计雇员未经允许偷偷留下的后门和生产、测试需要的附件。比如，一个保密的 CPU 使外界无法存储芯片内的某保密字，然而，设计者不公开的测试端口却保留了对此保密字的存取权。

因为网络拥有较为复杂的设备和协议，因此不能保证复杂的系统没有缺陷和漏洞。如 Windows NT 系统，没有任何人能全部地了解其每一细节，随着用户的增加，其 Bug 也不断被发现。Intel 的 MMX 芯片经过无数专家审核仍存在设计上的错误。系统设计的后门随着系统的复杂越来越难于发现。系统和软件工程学也告诉我们，大型系统将永远有令用户不满意的地方，直到此系统被停止使用，即生命终止。

网络的地域分布使得安全管理难于顾及网络连接的每个角落。

伴随着工业化的进程，任何网络拥有者或用户都不能单靠自己完全研制、开发、设计和制造网络的所有设备，组织大规模的开发和研制也无法保证每个人都忠于职守。网络是一个社会，社会大了，各种人都会有。有守法的，也有表面守法背后违法的。

没有人能证明网络是安全的。网络安全问题变为了一个风险管理问题，安全

性成为概率意义上无法准确定义的指标。合理地增加安全投资，增加正确的安全设备，改善安全管理，无疑可以提高网络的安全性能。

从攻击者的角度看，由于网络的复杂性与协议的多样性，攻击的投入越大，找到攻击入口和网络弱点的可能性也越大，攻击成功的机会也越大。如果攻击成功后的收益很大，则攻击者一般会投入较大的力量。

网络安全没有保障。使用网络带来效益也带来风险，正确增加安全投入就减少了风险，而错误的投入就如同投资迷信和神汉一样，不能减少风险。但在某阶段侥幸没有损失的可能性也是存在的。

网络安全的威胁同时来自于内外两个方面。有一段时间，人们把初期的防火墙保障安全的功能强调到了不适当的地位，给人一个错觉，好像安全威胁全部来自于诸如 Internet 这些公众环境，这其实是一种误解。

对我国而言，自 1994 年 Internet 发展至今，已发生多次规模性的因黑客攻击造成的网络安全事件。第一次发生于 1997 年印尼排华反华事件后；第二次发生于 1999 年 5 月，北约轰炸中国驻南联盟大使馆后；第三次发生在 1999 年 7 月李登辉公然抛出“两国论”之后；第四次发生在 2000 年初日本右翼公然为南京大屠杀翻案后；第五次发生在 2001 年 2~3 月，由于日本三菱事件、日航事件、松下事件、教科书事件和《台湾论》等引起；第六次发生在中美“撞机事件”后，因美国电脑黑客组织——POIZONBOX 的挑衅行为，激怒了许多中国的电脑黑客而引起，这次攻击事件在 2001 年 5 月 4 日左右达到高潮。在这次世界范围大规模的攻击事件过程中，我国共有千余个站点受到攻击和破坏，美国也有数百个网站被攻击破坏，这是近年来中国网络安全受到的最大挑战。

面对这些频频发生的安全挑战，人们不禁要问：我们的网络安全吗？中国的网络安全之路究竟应该怎样走？这需要安全法规、法律、策略、技术、工具、措施和服务等各方面的配合。在未来的信息社会，要掌握自己的命运，就必须在网络安全防护技术、网络安全人才和相关法律政策上构建自己的网上长城，建筑自己的安全体系。只有这样，才能保证国家信息系统处于安全状态，“信息化”才能真正为中国腾飞带来希望。

编者的话

本书取名《黑客攻击技术揭秘》，其宗旨是注重知识性和实用性，在回顾网络信息安全发展的基础上，总结了信息安全的特征，介绍了信息安全的分类与常见的网络攻击行为，对危害网络信息安全的黑客攻击技术进行了深入细致的分析、讲解，通过对常见网络攻击行为的分析，详细解剖危害网络信息安全的黑客攻击技术，在文字的表述上力求深入浅出、不落俗套。本书第1章在回顾网络信息安全发展的基础上，总结了信息安全的特征，第2章到第4章，按照网络信息系统安全问题作用点的分类方式，分别进行介绍和说明，叙述流畅易懂，具有教科书性质，使读者能够循序渐进，抓住网络信息安全关键因素。本书第5～12章分别介绍了当前常见的攻击手段与原理，包括黑客、入侵系统类攻击、欺骗类攻击、拒绝服务攻击、攻击防火墙、病毒攻击、木马程序攻击、信息战等，可让读者对黑客的攻击手法有一定的认识与辨别能力。该书对于网络信息安全专业技术人员及信息时代的创业者都不失为一本实用的工具书，并将引导广大读者登堂入室、步入佳境。本书内容翔实，颇具启发性。对于本书的读者和网络信息安全相关从业人员来说，应学会充实、修正原有的知识和材料，这样每个人都可以共享他人的经验，我们在本书中也尝试着这样做。

本书由许榕生主笔，刘宝旭、杨泽明主要编写，曾勇、吴海燕、郭立生、任金强、安德海、丁宇征、毕学尧、李雪莹、孙笑庆、崔石、姜力东、钱桂琼、高娜等参加了部分内容的编写。全书由许榕生统稿。

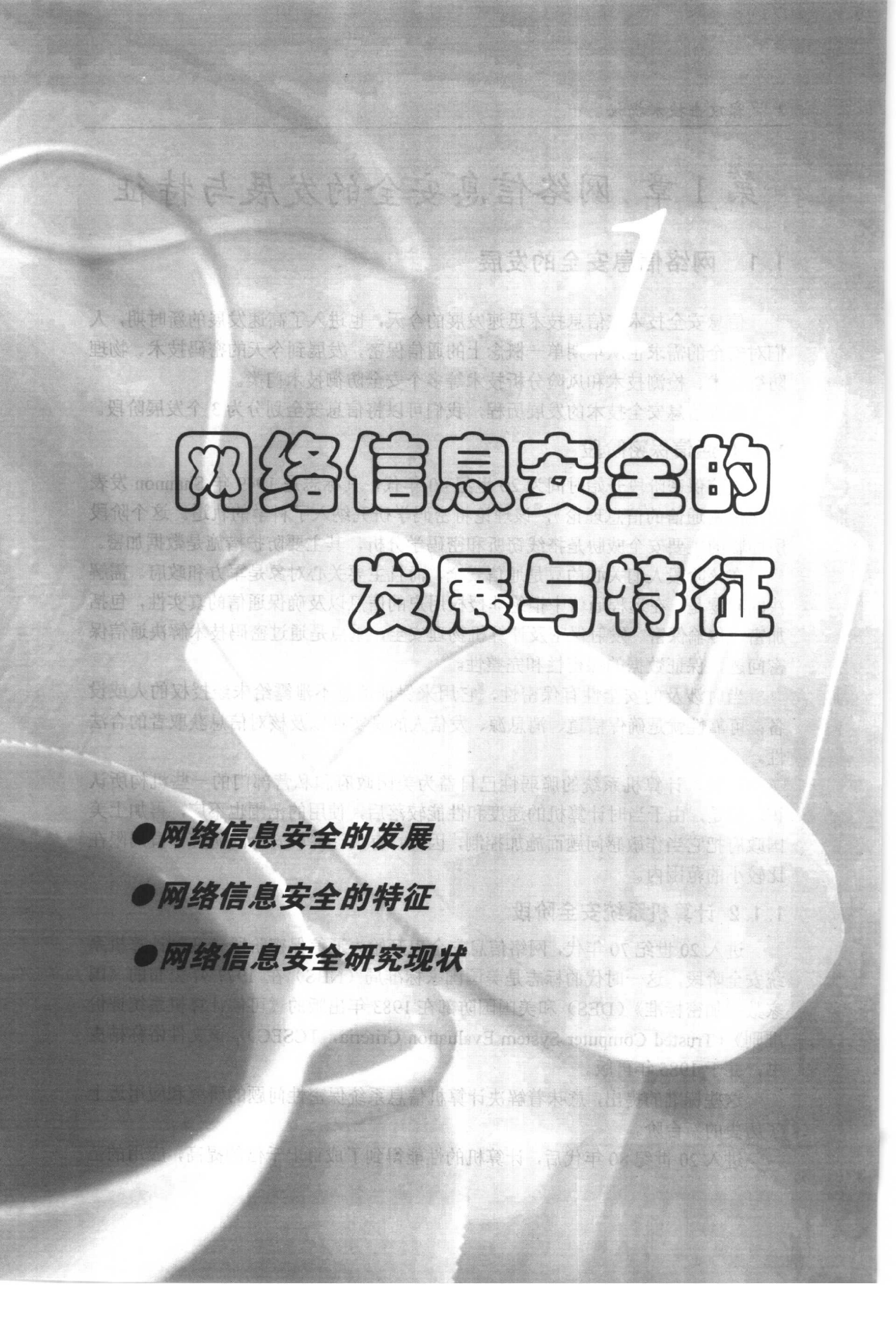
感谢中科院高能所计算中心网络安全课题组、国家计算机网络入侵防范中心、北京金元龙脉信息科技有限公司、北京中科网威信息技术有限公司、福建省海峡信息技术有限公司的各位同仁在提供资料、论文和录入编排方面所做的工作。

在本书写作过程中还得到了各方面专家和技术人员的支持和帮助，特别是参考引用了《中国计算机报》、《计算机世界》和许多互联网站上有关作者、编者、读者发表的观点和素材，恕不一一列举，在此一并表示感谢。

本书的创意要求坚持特色，集思广益。但由于时间仓促，错误与不妥之处在所难免，敬请广大读者谅解，并欢迎批评指正。

编　者

目　录



1 网络信息安全的发展与特征

- 网络信息安全的发展
- 网络信息安全的特征
- 网络信息安全研究现状

第 1 章 网络信息安全的发展与特征

1.1 网络信息安全的发展

信息安全技术在信息技术迅速发展的今天，也进入了高速发展的新时期，人们对安全的需求也从早期单一概念上的通信保密，发展到今天的密码技术、物理防御技术、检测技术和风险分析技术等多个安全防御技术门类。

纵观信息安全技术的发展历程，我们可以将信息安全划分为 3 个发展阶段。

1.1.1 通信保密阶段

通信保密阶段开始时间为 20 世纪 40 年代，其标志是 1949 年 Shannon 发表的《保密通信的信息理论》，该理论将密码学研究纳入了科学的轨道。这个阶段所面临的主要安全威胁是搭线窃听和密码学分析，其主要防护措施是数据加密。

在该阶段人们关心的只是通信安全，而且主要关心对象是军方和政府。需解决的问题是，在远程通信中拒绝非授权用户的信息以及确保通信的真实性，包括加密、传输保密、发射保密及计算机物理安全，重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。

当时涉及的安全性有保密性，它用来保证信息不泄露给未经授权的人或设备；可靠性就是确保信道、消息源、发信人的真实性以及核对信息获取者的合法性。

当时，计算机系统的脆弱性已日益为美国政府和私营部门的一些机构所认识。但是，由于当时计算机的速度和性能较落后，使用的范围也不广，再加上美国政府把它当作敏感问题而施加控制，因此，有关计算机安全的研究一直局限在比较小的范围内。

1.1.2 计算机系统安全阶段

进入 20 世纪 70 年代，网络信息安全也开始由通信保密阶段转变到计算机系统安全阶段，这一时代的标志是美国国家标准局（NBS）在 1977 年公布的《国家数据加密标准》（DES）和美国国防部在 1983 年出版的《可信计算机系统评价准则》（Trusted Computer System Evaluation Criteria，TCSEC），该文件俗称桔皮书，并于 1985 年再版。

这些标准的提出，意味着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。

进入 20 世纪 80 年代后，计算机的性能得到了成百上千倍的提高，应用的范

围也在不断扩大，计算机已遍及世界各个角落。并且，人们利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题。人们在这方面所做的研究，与计算机性能和应用的飞速发展不相适应，因此，它已成为未来信息技术中的主要问题之一。

由于计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，还有可能受到计算机病毒的感染。

该阶段的重点是确保计算机系统中的硬件、软件及在处理、存储、传输信息中的机密性、完整性和可控性。主要安全威胁已扩展到非法访问、恶意代码、脆弱口令等，主要保护措施是安全操作系统设计技术（TCB）。

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。”此概念偏重于静态信息的保护。也有人将“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的描述。

美国国防部（DOD）于 1985 年再版的《可信计算机系统的评价准则》（又称“桔皮书”），使计算机系统的安全性评估有了一个权威性的标准。DOD 的桔皮书中使用了可信计算基础（Trusted Computing Base，TCB）这一概念，即计算机硬件与支持不可信应用及不可信用户的操作系统的组合体。桔皮书将计算机系统的可信程度划分为 D、C1、C2、B1、B2、B3 和 A1 共 7 个层次。在 DOD 的评价准则中，从 B 级开始就要求具有强制存取控制和形式化模型技术的应用。桔皮书论述的重点是通用的操作系统，为了使它的评判方法适用于网络，美国国家计算机安全中心于 1987 年出版了《可信网络指南》。该书从网络安全的角度出发，解释了准则中的观点。

1.1.3 网络信息系统安全阶段

进入 20 世纪 90 年代后，网络信息安全的发展，开始由计算机系统安全阶段转变到网络信息系统安全阶段，这一时代网络信息安全的主要标志是：提出了新的安全评估准则 CC（ISO 15408）、IPV6 安全性设计等安全标准和安全协议。重点需要保护信息，确保信息在存储、处理、传输过程中信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击措施，强调信息的保密性、完整性、可控性、可用性；主要安全威胁已发展到网络入侵、病毒破坏和信息对抗的攻击等；主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI 和 VPN。网络信息安全分为系统安全、信息安全和文化安全，如图 1-1 所示。

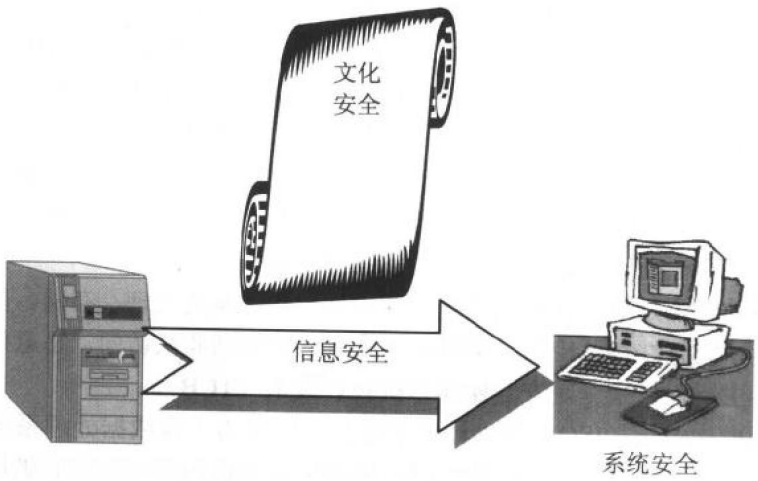


图 1-1　安全层面分析示意图

所谓的系统安全，其作用点为对计算机网络与计算机系统可用性的威胁，主要表现在访问控制方面。外部表现为网络被阻塞、黑客行为和计算机病毒等，它使得依赖于信息系统的管理或控制体系陷于瘫痪。主要的防范措施包括防止入侵、检测入侵、抵抗入侵和系统恢复。

信息安全的主要作用点，是对所处理的信息机密性与完整性的威胁，主要表现在加密方面。其外部表现为窃取信息、篡改信息、冒充信息和信息抵赖等；防范措施包括加密、认证、数字签名和完整性技术等，如图 1-2 所示。

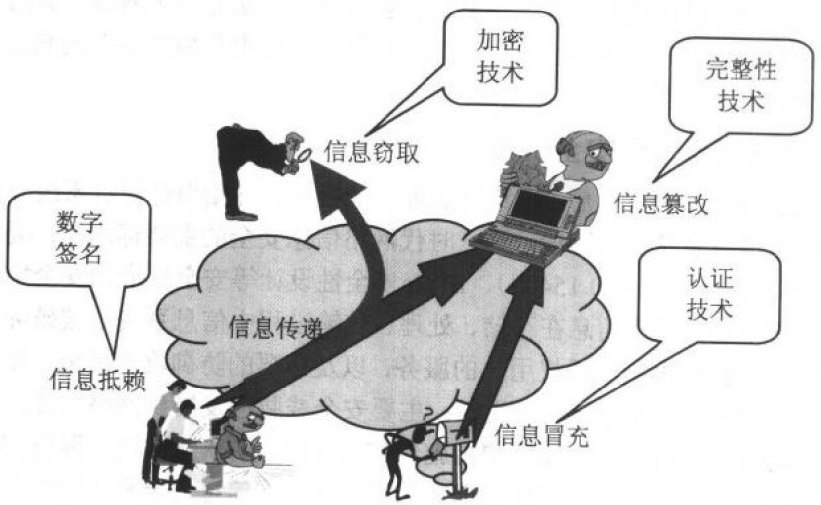


图 1-2　信息安全分析示意图

文化安全的主要作用点是有害信息的传播对我国的政治制度及文化传统的威胁，主要表现在舆论宣传方面。其外部表现主要为：黄色、反动信息泛滥；敌对的意识形态信息涌入；互联网被利用作为串联工具；传播迅速；影响范围广。防范措施包括：设置因特网网关、监测和控管等，如图 1-3 所示。

20 世纪 90 年代以来，通信和计算机技术相互依存，数字化技术促使计算机网络发展成为全天候、通全球、个人化和智能化的信息高速公路，Internet 成了寻常百姓的家用信息平台，信息安全的概念随之产生，安全的需求不断地向社会的各个领域扩展。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改，以及确保对合法用户的服务和限制非授权用户的服务，包括必要的检测、记录和抵御攻击的措施。

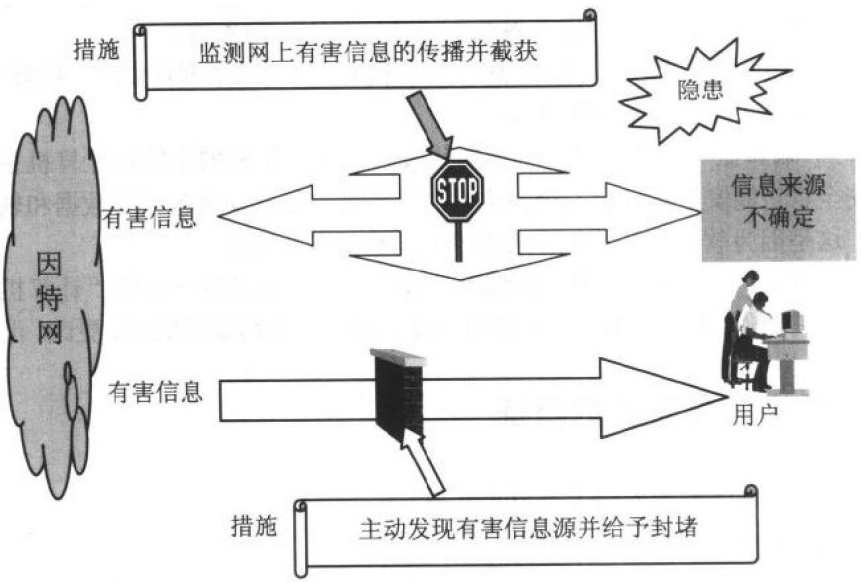


图 1-3 文化安全分析示意图

此时对安全性有了新的需求：可控性（Controllability），即对信息及信息系统实施安全监控管理；不可否认性（Non－repudiation），即保证行为人不能否认自己的行为。

此时期，在密码学方面，公开密钥密码技术得到了长足的发展，著名的 RSA 公开密钥密码算法获得了日益广泛的应用，用于完整性校验的 Hash 函数的研究应用也越来越多。为了奠定 21 世纪的分组密码算法基础，美国国家技术标准研究所（NIST）推行了高级加密标准（AES）的项目，并于 1998 年 7 月选出了 15 种分组密码算法作为候选算法。目前，经过广泛评价，已进一步从中选出了 5 个

较好的算法，并在上世纪末选出惟一的 AES 算法。而更强更快的公开密钥密码算法研究和应用，则把希望寄托在椭圆曲线公开密钥密码算法上。目前安全威胁已发展到黑客的网络入侵、病毒破坏和计算机犯罪事件等程度。

时至今日，对于信息系统的攻击日趋频繁，安全的概念已经不再局限于信息的保护，人们需要的是对整个信息和信息系统的保护和防御，以确保它们的安全性，包括了对信息的保护、检测、反应和恢复能力（PDRR）。这就是信息安全保障的概念：为了保障信息安全，除了要进行信息的安全保护，还应该重视提高系统的入侵检测能力，系统的事件反应能力和系统遭到入侵引起破坏的快速恢复能力。区别于传统的加密、身份认证、访问控制、防火墙和安全路由等技术，信息保障强调信息系统整个生命周期的防御和恢复。

国外自 20 世纪 60 年代即开始了计算机安全研究与实践，并逐渐形成了比较定型的概念。目前国际上对安全概念主要流行如下 3 种流派。

（1）美国派　美国流行的认识，认为计算机安全即指硬件安全、软件安全、通信（或网络）安全和数据安全等。

（2）瑞典派　瑞典是另一学派的代表，认为计算机安全即指计算机系统的实体安全、功能安全和信息安全，认为在计算机中信息安全包括了数据和软件的安全，这是因为软件在计算机中表现形式与数据并无两样。

（3）ISO 派　国际标准化组织对计算机安全曾做过统一建议“计算机系统应该保护其硬件、软件与数据，不因偶然或故意的原因而遭到破坏、更改、泄露”。

1.2　网络信息安全的特征

网络信息安全的主要特征有以下几点。

1.2.1 相对性

安全只是相对的，世上没有绝对的安全系统。安全将是网络永恒的问题，风险是无法完全消除的，零风险就意味着网络的零效用，关键的问题是如何达到均衡，即尽可能地降低风险，又使网络发挥其最大效用。

从网络信息系统（Network Information System，简称“NIS”）集成的角度看，使用商业成品设备和技术（Commercial Off-the Shelf，简称“COTS”）可能比完成自主开发的软件安全性更好，因此一个实际的 NIS 不可能排除 COTS 产品。

安全性在系统的不同部件之间可以转移（如在内部网络和外部网络之间使用堡垒主机），这样可以使用非可信部件组成可信系统（不遵循可靠性理论中的“木桶理论”）。