ISBN 7-111-09886-2/TP·2322
选题策划：边　萌
封面设计：樊　俊

21世纪网络工程丛书——安全防卫系列

黑客攻击技术揭秘

黑客防范技术揭秘

阻击黑客进攻防卫技术

黑客入侵防护系统源代码分析

ISBN 7-111-09886-2
9 787111 098867 >

地址：北京市百万庄大街22号
电话：68326335　邮编：100037
http://www.cmpbook.com
E-mail:online@cmpbook.com

定价：29.00元（附1CD）

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）

目 录

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。

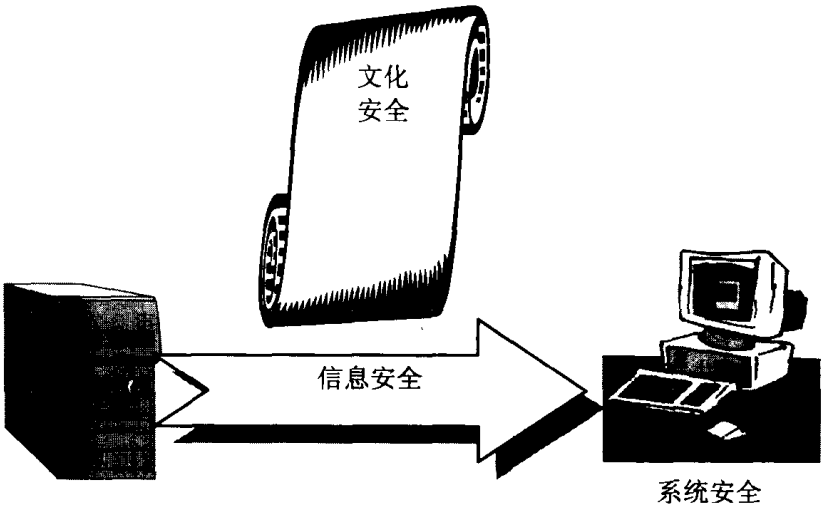


图 1-1　安全层面分析示意图

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。

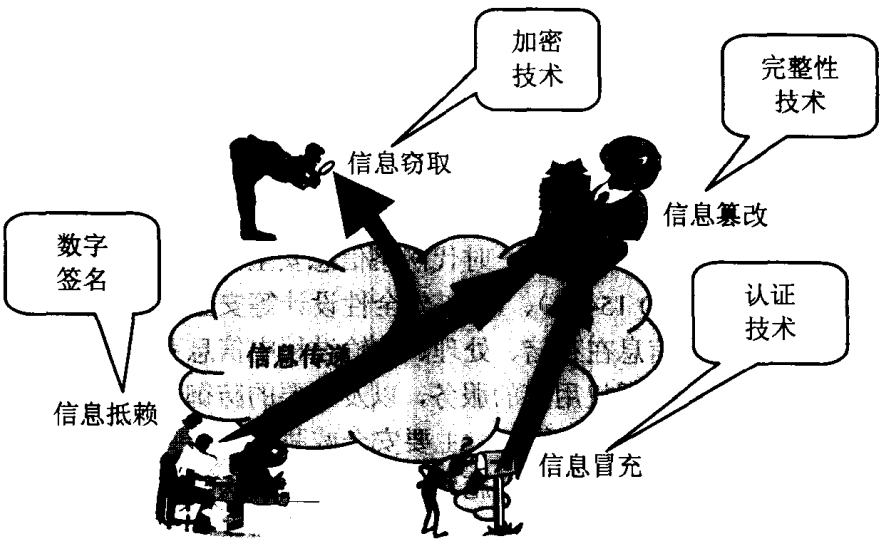


图 1-2　信息安全分析示意图

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。

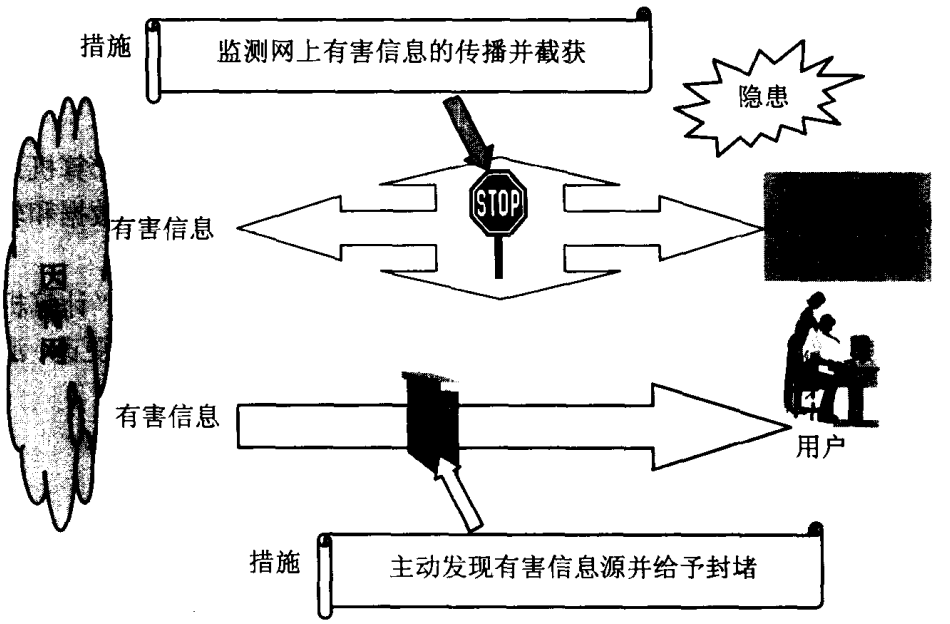


图 1-3 文化安全分析示意图

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”）。

1.2.2 攻击的不确定性

网络遍布世界各地，网络用户群越来越庞大，接入越来越方便。所以，在任何时间、任何地点，任何人都可以对网络发起攻击，这便导致网络信息安全具有很强的不确定性。

1.2.3 复杂性

信息安全是一项系统工程，需要技术的与非技术的手段，涉及到人的因素，涉及很多技术层面，涉及安全管理、教育、国际合作与互不侵犯协定、培训、立法和应急反应等诸多环节，所以，网络信息安全具有复杂性。

1.2.4 时效性

新的漏洞与攻击方法不断被发现，使得网络安全具有明显的时效性。

整个网络信息安全系统应尽可能引入更多的可变因素，并具有良好的扩展性。

如果加密信息在被破译之前就失去了保密的必要性，即使加密算法不是牢不可破的，被保护的信息也是安全的。因此，被加密信息的生存期越短、可变因素越多，系统的安全性就越高，如周期性的更换口令和主密钥、采用一次性会话密钥、动态选择和使用加密算法等。另一方面，各种密码攻击和破译手段在不断发展，用于破译运算的资源和设备性能也在迅速提高，网络设备与构架及应用系统也在不断变化，因此，所谓的安全，也只是相对的和暂时的，不存在一劳永逸的网络信息安全系统，安全系统必须根据攻击手段的发展进行相应的更新和升级。

1.2.5 配置相关性

日常管理中的不同配置会引入新的问题（安全评估只证明特定环境与特定配置下的安全）。新的系统部件也会引入新的问题。

1.2.6 动态性

网络的地域分布使得安全管理难于顾及网络连接的各个角落，所以，没有人能证明或保证网络是安全的，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，安全又成为一个动态意义上的概念。

由此，有人给出计算机网络安全的如定义：“计算机网络安全指其硬件、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”。

网络设备和软件不可能是完美的，在设计开发过程中必然会存在某些缺陷和漏洞。这些漏洞和缺陷恰恰是隐患存在的主要环节。网络信息系统的安全漏洞是动态出现的，日常管理中的不同配置会引入新的问题，新的系统部件也会引入新

的问题。因此，网络安全漏洞和隐患是动态发展的。

1.3 网络信息安全研究现状

网络安全（又称信息安全）的发展经历了一个漫长的阶段，并于 20 世纪 90 年代以来得到了深化，从信息的保密性（保证信息不泄漏给未经授权的人），拓展到信息的完整性（防止信息被未经授权的人篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、信息的可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝管理）、信息的不可否认性（保证信息行为人不能否认自己的行为）等。信息安全需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

国际上信息安全研究起步早、力度大、积累多、应用广。20 世纪 80 年代，美国国防部基于军事计算机系统的保密需要，在 20 世纪 70 年代的基础理论研究成果—计算机保密模型（Bell & La Padula 模型）的基础上，制订了“可信计算机系统安全评价准则”（TCSEC），其后又制订了关于网络系统、数据库等方面的准则和系列安全解释，形成了安全信息系统体系结构的最早原则。

至今美国已研究出达到 TCSEC 要求的安全系统（包括安全操作系统、安全数据库、安全网络部件）产品达 100 多种。

20 世纪 90 年代初，英国、法国、德国和荷兰 4 个国家针对 TCSEC 准则只考虑保密性的局限，联合提出了包括保密性、完整性和可用性概念的“信息技术安全评价准则”（TISFC），但是该准则中并没有给出综合解决以上问题的理论模型和方案。

近年来六国七方（美国国家安全局和国家技术标准研究所、加拿大、英国、法国、德国、荷兰）共同提出了“信息技术安全评价通用准则”（CC for IT SEC）。

它综合了国际上已有的评审准则和技术标准的精华，给出了框架和原则要求。然而，将它作为取代 TCSEC 用于系统安全评测的国际标准，仍然缺少综合解决信息的多种安全属性的理论模型依据。同时，他们的高安全级别的产品对我国是封锁禁售的。

安全协议作为信息安全的重要内容，其形式化方法分析始于 20 世纪 80 年代初，目前有基于状态机、模态逻辑和代数工具的 3 种分析方法，但仍有局限性和漏洞，还处于发展提高阶段。

由于在广泛应用的国际互联网上，黑客入侵事件不断发生，不良信息大量传播，因此网络安全监控管理理论和机制的研究受到重视，黑客入侵手段的研究分析、系统脆弱性检测技术、报警技术、信息内容分级标识机制和智能化信息内容分析等研究成果，已经成为众多安全工具软件的基础。

研究中揭示出系统中存在许多设计缺陷，存在情报机构有意埋伏的安全陷阱的可能。

例如在 CPU 芯片中，在发达国家现有技术条件下，可以植入无线发射接收功能，在操作系统、数据库管理系统或应用程序中，能够预先安置从事情报收集、受控激发的破坏程序。

通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CPU 的自杀功能，搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过惟一识别 CPU 个体的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先设定收集敏感信息或进行定向破坏。

作为信息安全关键技术的密码学，近年来空前活跃。美、欧、亚各洲举行的密码学和信息安全学术会议十分频繁。

1976 年美国学者提出的公开密钥密码体制克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，并可用于身份认证，它是当前研究的热点。电子商务的安全性是当前人们普遍关注的焦点，目前正处于研究和发展阶段，它带动了论证理论、密钥管理等的研究。

1977 年美国颁布使用的国家数据加密标准由于密码分析和攻击手段的进步，已不能满足安全需要，美国正在征集作为 21 世纪的新的数据加密标准。计算机运算速度的不断提高，各种密码算法面临着新的密码体制如量子密码、DNA 密码、混沌理论，正处于探索中。

基于密码理论的综合研究成果和可信计算机系统的研究成果，构建公开密钥基础设施，密钥管理基础设施成为当前的另一个热点。

我国的信息安全研究经历了通信保密和计算机数据保护两个发展阶段，目前正进入网络信息安全的研究阶段。

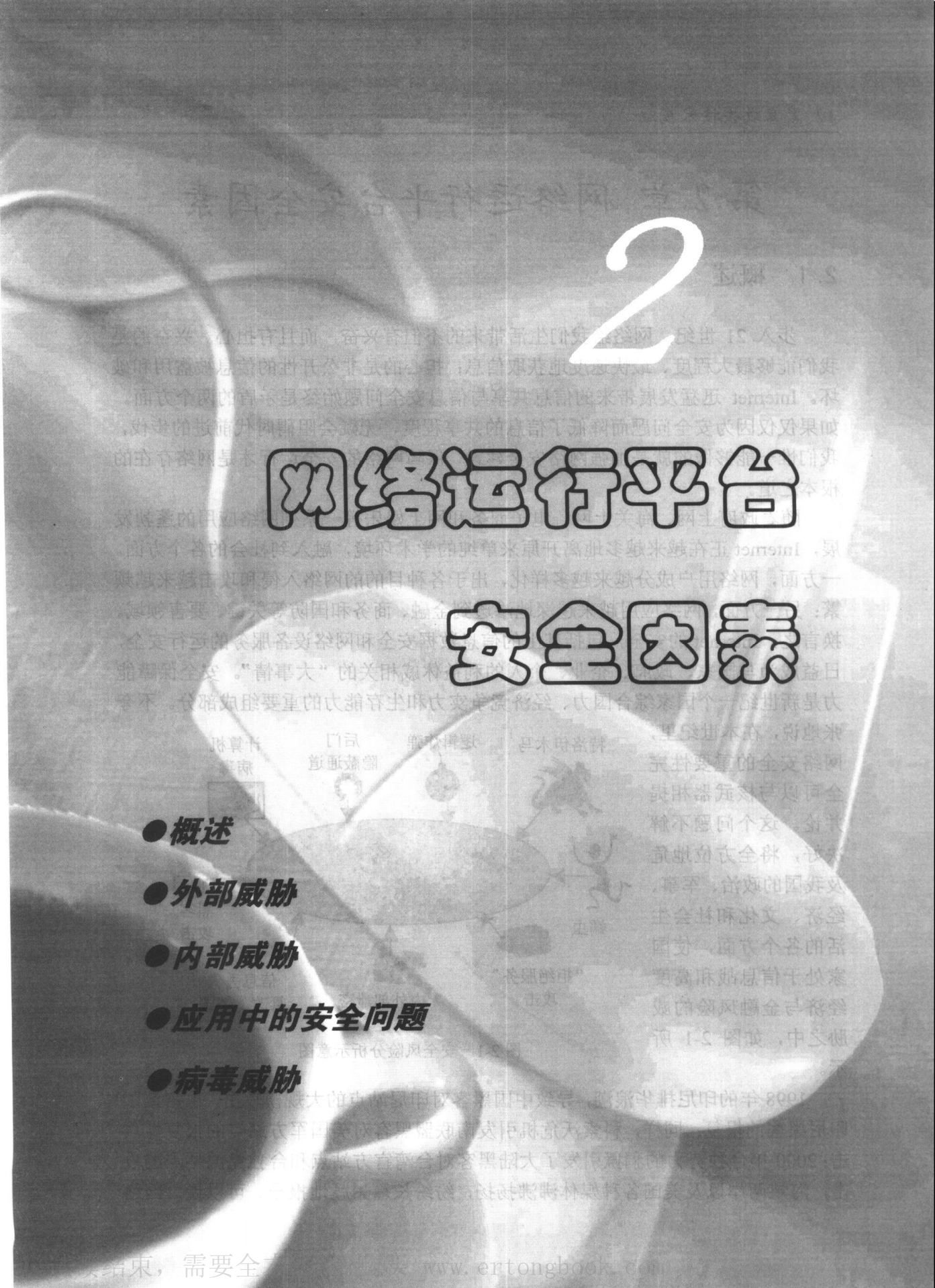
通过学习、吸收和消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新、升级，因此基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广应用。

在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测和系统脆弱性扫描软件等。但是，这些产品安全技术的完善性、规范化和实用性还存在许多不足，特别是在多平台的兼容性、多协议的适应性和多接口的满足性方面还存在很大距离，理论基础和自主的技术手段也需要发展和强化。

总的来说，我国的网络信息安全研究起步晚、投入少、研究力量分散，与技术先进国家有差距，特别是在系统安全和安全协议方面的工作与国外差距更大。

在我国研究和建立创新性安全理论和系列算法，仍是一项艰巨的任务。然而

我国的网络信息安全研究毕竟已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，只要国家重视，加大投入，恰当组织，完全可以取得实质性进展。



2 网络运行平台安全因素

- 概述
- 外部威胁
- 内部威胁
- 应用中的安全问题
- 病毒威胁