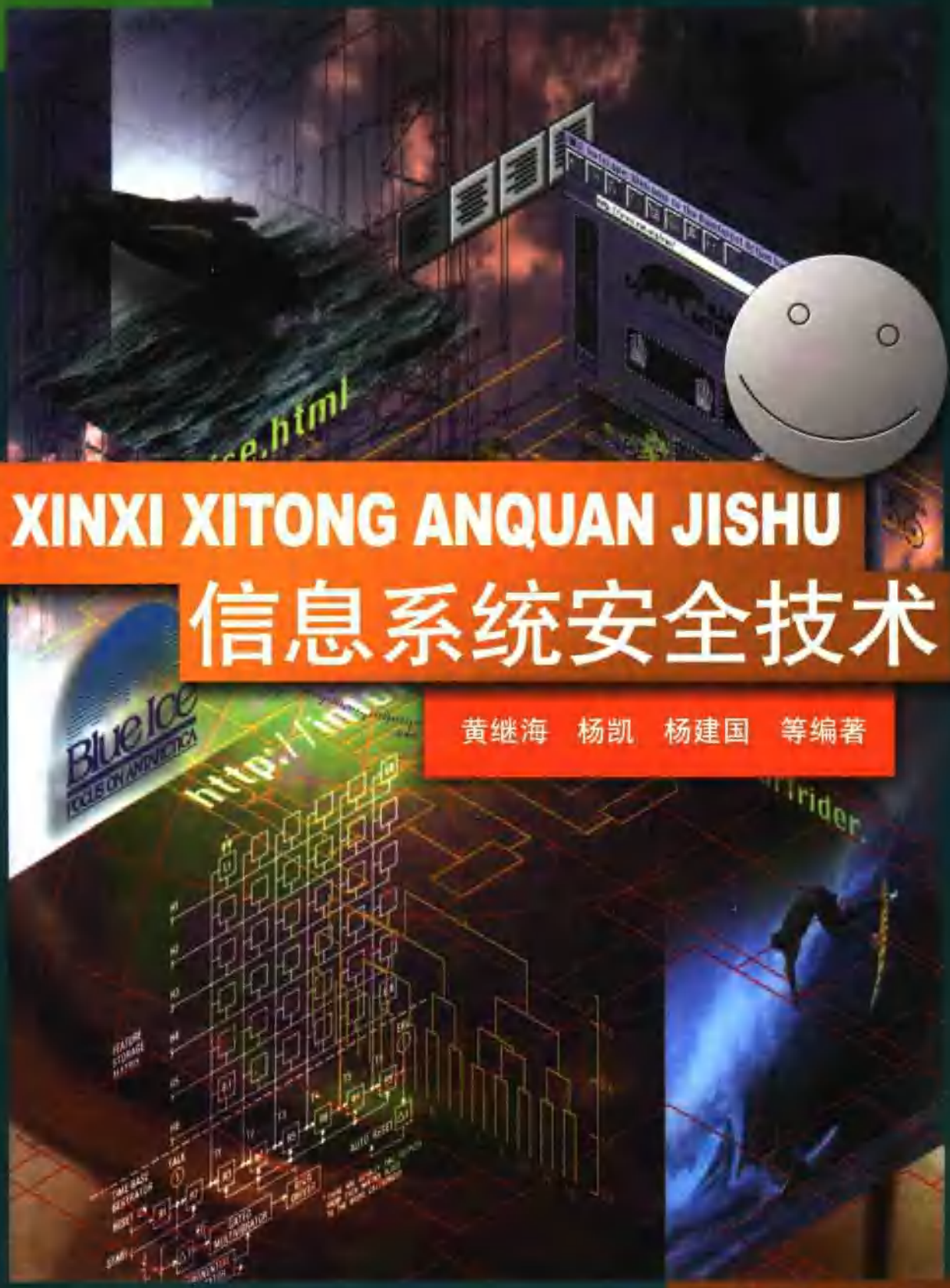

XINXI XITONG ANQUAN JISHU

信息系统安全技术

黄继海　杨凯　杨建国　等编著

河南科学技术出版社

信息系统安全技术

黄继海
杨　凯　等编著
杨建国

河南科学技术出版社
·郑州·

内　容　简　介

本书从计算机泄密途径和我国网络信息安全现状入手，介绍了信息安全和网络安全技术的基本知识，涉及身份认证技术、常用加密算法、访问控制技术、入侵检测技术、防病毒技术、网络隔离、防火墙技术、安全扫描技术和安全审计技术等网络信息安全体系，并详细讲解了指纹和声纹等高科技加密手段。实际指导架设 Linux 下的 VPN 安全系统，分析黑客常用的网上攻击方法针对性采用先进的防护手段保障网络安全，同时对操作系统的安全和网站建设的安全问题进行系统地研究和方案设计。以实际案例较为全面地介绍了现代流行的信息安全技术。

本书注重理论和实践相结合，内容实用、层次分明、语言流畅，所涵盖的内容对大家提高网络安全意识和主动进行网络安全防护是不可或缺的。

阅读本书的读者应具备基本的计算机网络知识。本书可以作为计算机类专业或信息类相关专业的本科或专科教材，也可供从事计算机网络开发和安全研究的科研人员参考，同时可以作为一本网络安全手册。

图书在版编目（CIP）数据

信息系统安全技术/黄继海等编著. —郑州：河南科学技术出版社，2006.2
ISBN 7-5349-3455-9

Ⅰ.信…　Ⅱ.黄…　Ⅲ.信息系统-安全技术　Ⅳ.TP309

中国版本图书馆CIP数据核字（2006）第005649号

出版发行：河南科学技术出版社
地址：郑州市经五路66号　邮编：450002
电话：（0371）65737028
责任编辑：张晓东
责任校对：柯　姣
封面设计：张　伟
版式设计：栾亚平
印　　刷：河南第一新华印刷厂
经　　销：全国新华书店
幅面尺寸：185 mm×260 mm　印张：13.75　字数：400千字
版　　次：2006年2月第1版　2006年2月第1次印刷
印　　数：1—4100
定　　价：28.00元

前　言

《信息系统安全技术》编写人员

编　著　黄继海　杨　凯　杨建国　于政庆
　　郎士宁　孟　军　李宝林　王　辉

审　稿　左　军

目 录

第 1 章

网络信息安全概论

当今社会，信息化的浪潮正在迅速渗透到全球的各个领域。信息化是一把双刃剑。它在为我们带来巨大便利的同时，也留下了信息安全隐患。随着信息网络的飞速发展，信息网络的安全防护技术已逐渐成为一个新兴的重要技术领域，并且受到政府、军队和全社会的高度重视。随着我国政府、金融等重要领域逐步进入信息网络，国家的信息网络已成为继领土、领海、领空之后的又一个安全防卫领域，逐渐成为国家安全的最高价值目标之一。可以说信息网络的安全与国家安全密切相关。

网络的发展已经深入到社会生活的各个方面。对个人而言，网络改变了人们的生活方式；对企业而言，网络改变了企业传统的营销方式及其内部管理机制；对军事而言，网络引起了军事思想、军事理论和作战模式的变革。虽然一切便利都源于网络，但是一切安全隐患也源于网络。网络设计之初，只考虑到相互的兼容和互通，并没有考虑到随之而来的一系列安全问题，这就使网络安全伴随网络的发展而不断发展。网络新业务的不断兴起，如电子商务、数字货币、网络银行、军事上的信息作战等，对网络安全提出了更高的要求。黑客入侵案件不断发生，给我们敲响了警钟，同时也给我国网络安全提出了严峻的挑战。21 世纪是网络信息安全的世纪，信息获取能力和信息安全保障能力是当今世界各国政府和军队奋力抢占的制高点。目前我国使用的交换机、路由器等网络互联设备几乎都是国外的产品，一些国内的应用系统也是建立在国外操作系统的基础之上的。所以，如何在这片沙滩上建立起我国自主的网络信息安全保障体系堡垒，是亟待解决的问题。随着网络的发展，计算机网络的安全保密问题已经成为日益严峻的现实问题，因此研究网络安全有着重要的意义。

1.1 计算机泄密的主要途径

计算机泄密的主要途径包括计算机电磁波辐射泄漏、计算机网络化造成的泄密、计算机媒体泄密、内部工作人员泄密。

1.1.1 计算机电磁波辐射泄漏

计算机电磁波辐射泄漏一类是传导发射，通过电源线和信号线辐射，另一类是由于设各中的计算机处理机、显示器有较强的电磁辐射。计算是靠高频脉冲电路工作的，由

于电磁场的变化，必然要向外辐射电磁波。这些电磁波会把计算机中的信息带出去，感兴趣的人只要具有相应的接收设备，就可以将电磁波接收，从中窃得秘密信息。据国外试验，在 1 000 米以外能接收和还原计算机显示终端的信息，而且看得很清晰。计算机工作时，在开阔地带距其 100 米外，用监听设备就能收到辐射信号。从计算机的运算器和控制器及外部设备等部分辐射，频率一般在 10 兆赫到 1 000 兆赫范围内，这种电磁波可以用相应频段的接收机接收，但其所截信息解读起来比较复杂。由计算机终端显示器的阴极射线管辐射出的视频电磁波，其频率一般在 6.5 兆赫以下。对这种电磁波，在有效距离内，可用普通电视机或相同型号的计算机直接接收。接收或解读计算机辐射的电磁波，现在已成为国外情报部门的一项常用窃密技术，并已达到很高水平。

1.1.2 计算机网络化造成的泄密

目前，网络是计算机信息安全问题存在的主要地方，安全问题主要表现为网络运行安全、信息内容的安全、内容管理安全、服务器系统安全、网络操作安全等方面的问题。网络不安全的原因表现在网络自身的缺陷、网络的开放性以及黑客的攻击。具体表现在以下诸多方面。

（1）由于计算机网络结构中的数据是共享的，主机与用户之间、用户与用户之间通过线路联络，就存在许多泄密漏洞。计算机联网后，传输线路大多由载波线路和微波线路组成，这就使计算机泄密的渠道和范围大大增加。网络越大，线路通道分支就越多，输送信息的区域也越广，截取所送信号的条件就越便利，窃密者只要在网络中任意一条分支信道上或某一个节点、终端进行截取，就可以获得整个网络输送的信息。

（2）黑客通过利用网络安全中存在的问题进行网络攻击，进入联网的信息系统进行窃密，对数据进行破坏和篡改等。

（3）Internet 上造成的泄密。如在 Internet 上发布信息把关不严；Internet 用户在 BBS、网络新闻组上谈论国家秘密事项等；使用 Internet 传送国家秘密信息造成国家秘密被窃取；内部网络连接到 Internet 遭受窃密者从 Internet 攻击进行窃密；处理涉密信息的计算机系统没有与 Internet 进行物理隔离，使系统受到国内外黑客的攻击。

（4）间谍组织通过 Internet 搜集、分析、统计国家秘密信息。如在 Internet 上，利用特洛伊木马技术对网络进行控制，如 BO、BO2000。

（5）网络管理者安全保密意识不强，造成网络管理的漏洞。

1.1.3 计算机媒体泄密

越来越多的秘密数据和档案资料被存储在计算机里，大量的秘密文件和资料变为磁性介质和光学介质，存储在无保护的介质里，媒体的泄密隐患相当大。常见的泄密途径有以下几种。

（1）使用过程的疏忽和不懂技术。存储在媒体中的秘密信息在联网交换的过程中被泄露或被窃取，存储在媒体中的秘密信息在进行人工交换时泄密。

（2）大量使用的磁盘、磁带、光盘等外存储器很容易被复制。

（3）处理废旧磁盘时，由于磁盘经消磁十余次后，仍有办法恢复原来记录的信息，

存有秘密信息的磁盘很可能被利用磁盘剩磁提取原记录的信息。这很容易发生在磁盘报废时或存储过秘密信息的磁盘，用户认为已经清除了信息，而给其他人使用。

（4）计算机出故障时，存有秘密信息的硬盘不经处理或无人监督就带出修理，或修理时没有懂技术的人员在场监督，而造成泄密。

（5）媒体管理不规范。秘密信息和非秘密信息放在同一媒体上，明密不分。磁盘不标密级，不按有关规定管理载有秘密信息的媒体，容易造成泄密。

（6）媒体失窃。存有秘密信息的磁盘等媒体被盗，就会造成大量的国家秘密外泄，其危害程度将是难以估量的。各种存储设备存储量大，丢失后造成的后果非常严重。

（7）设备在更新换代时没有进行技术处理。如没有进行彻底地消磁或按密级存放。

1.1.4　内部工作人员泄密

1. 无知泄密

如由于不知道计算机的电磁波辐射会泄露秘密信息，计算机工作时未采取任何措施，因而给他人提供窃密的机会。又如由于不知道计算机软盘上剩磁可以提取还原，将曾经存储过秘密信息的软盘交流出去或不作任何技术处理而报废丢弃，因而造成泄密。不知道在连接上 Internet 时，会造成存在本地机上的数据和文件被黑客窃走。网络管理者缺乏安全保密知识。

2. 违反规章制度泄密

如将一台发生故障的计算机送修前既不做消磁处理，又不安排专人监修，造或秘密数据被窃。又如由于对计算机媒体存储的内容重视程度不够因而思想麻痹，疏于管理，造成媒体的丢失。违反规定把用于处理秘密信息的计算机，同时作为上 Internet 的机器。使用 Internet 传递国家秘密信息等。

3. 故意泄密

外国情报机关常常采用金钱收买、色情引诱和策反别国的计算机工作人员，窃取信息系统的秘密。如程序员和系统管理员被策反，就可以得知计算机系统软件保密措施，获得使用计算机的口令或密钥，从而打人计算机网络，窃取信息系统、数据库内的重要秘密；操作员被收买，就可以把计算机保密系统的文件、资料向外提供。维修人员被威胁引诱，就可利用进入计算机机房或接近计算机终端的机会，更改程序，装置窃听器等。

1.2　我国网络信息安全现状

1.2.1　软件和硬件设备上严重依赖国外，安全技术有待研究

我国信息化建设过程中缺乏自主技术支撑。缺乏自主的计算机网络和软件核心技术。计算机安全存在三大黑洞：CPU 芯片、操作系统和数据库、网关软件，它们大多依赖进口。信息安全专家点出我国信息系统的要害：我们的网络发展很快，但安全状况如何？现在有很多人投很多钱去建网络，实际上并不清楚它只有一半根基，建的是没有防

范的网。有的网络顾问公司建了很多网，但建的是裸网，没有保护，就像房产公司盖了很多楼，门窗都不加锁就交付给业主去住。我国计算机网络所使用的网管设备和软件基本上是舶来品，这些因素使我国计算机网络的安全性能大大降低，被认为是易窥视和易打击的“玻璃网”。由于缺乏自主技术，我国的网络处于被窃听、干扰、监视和欺诈等多种信息安全威胁中，网络安全处于极脆弱的状态。

1.2.2 网络安全管理存在漏洞

运行管理机制的缺陷和不足制约了安全防范的力度。运行管理是过程管理，是实现全网安全和动态安全的关键。有关信息安全的政策、计划和管理手段等最终都会在运行管理机制上体现出来。就目前的运行管理机制来看，有以下几方面的缺陷和不足。

一、网络安全管理方面人才匮乏

由于网络通信成本极低，分布式客户服务器和不同种类配置的网络不断出新和发展。但是技术应用的扩展，却忽略了技术管理的同步扩展，从事系统管理的人员往往并不具备安全管理所需的技能、资源和利益导向。信息安全技术管理方面的人才无论是数量还是水平，都无法适应信息安全形势的需要。

二、安全措施不到位

网络越来越具有综合性和动态性特点，这同时也是网络存在不安全因素的原因所在。然而，网络用户对此缺乏认识，未进入安全就绪状态就急于操作，结果导致敏感数据暴露，使系统遭受风险。配置不当或过时的操作系统、邮件程序和内部网络都存在入侵者可利用的缺陷，如果缺乏周密有效的安全措施，就无法及时发现和查堵安全漏洞。当厂商发布补丁或升级软件来解决安全问题时，许多用户的系统因管理者未充分意识到网络不安全的风险所在，不进行同步升级，造成安全隐患。

三、缺乏综合性的解决方案

面对复杂的不断变化的网络世界，大多数用户缺乏综合性的安全管理解决方案，稍有安全意识的用户越来越依赖“银弹”方案(如防火墙和加密技术)，但这些用户也就此产生了虚假的安全感，渐渐丧失警惕。实际上，一次性使用一种方案并不能保证系统一劳永逸和高枕无忧，网络安全问题远远不是防病毒软件和防火墙能够解决的，也不是大量标准安全产品简单堆砌就能解决的。近年来，国外的一些网络安全产品厂商及时应变，由防病毒软件供应商转变为企业安全解决方案的提供者。他们相继在我国推出多种全面的企业安全解决方案，包括风险评估和漏洞检测、入侵检测、防火墙和虚拟专用网、防病毒和内容过滤解决方案，以及企业管理解决方案等一整套综合性安全管理解决方案。

四、缺乏制度化的防范机制

不少单位没有从管理制度上建立相应的安全防范机制，在整个运行过程中，缺乏行之有效的安全检查和应对保护制度。不完善的制度滋长了网络管理者和内部人士自身的违法行为。许多网络犯罪行为(尤其是非法操作)都是因为内部联网电脑和系统管理制度疏于完善而得逞的。同时，政策法规难以适应网络发展的需要，信息立法还存在相当多的空白。个人隐私保护法、数据库保护法、数字媒体法、数字签名认证法、计算机犯罪

法以及计算机安全监管法等信息空间正常运作所需的配套法规尚不健全。由于网络作案具有手段新、时间短、不留痕迹等特点，给侦破和审理网上犯罪案件带来极大困难。

五、网络安全问题还没有引起人们的广泛重视

安全意识淡薄是加强网络安全的瓶颈。目前，在网络安全问题上还存在不少认知盲区和制约因素。网络是新生事物，许多人一接触就忙着用于学习、工作和娱乐等，对网络信息的安全性无暇顾及，安全意识相当淡薄，对网络信息不安全的事实认识不足。与此同时，网络经营者和机构用户注重的是网络效应，对安全领域的投人和管理远远不能满足安全防范的要求。

总体上看，网络信息安全处于被动的封堵漏洞状态，从上到下普遍存在侥幸心理，没有形成主动防范、积极应对的全民意识，更无法从根本上提高网络监测、防护、响应、恢复和抗打击能力。近年来，国家和各级职能部门在信息安全方面已做了大量努力，但就范围、影响和效果来讲，迄今所采取的信息安全保护措施和有关计划还不能从根本上解决目前的被动局面，整个信息安全系统在迅速反应、快速行动和预警防范等主要方面，缺乏方向感、敏感度和应对能力。

六、美国和西方国家对我国进行破坏、渗透和污染

不同文化、文明之间的矛盾，尤其是某些强势文化的渗人将危及中国的文化安全。当今网络上 90%的信息是英语信息，中文信息仅占 10%。语言的霸权常常意味着信息和文化的霸权。网络时代的信息霸权和强势文化的冲击使网络文化交流失去了平等交互性，变成了单向渗透。以美国为首的西方国家占据了网络传播的制高点，向中国大量传播带有其政治模式、价值观念和生活方式的各类信息，以反对和瓦解社会主义价值观。尤其是所谓宗教文化、色情暴力文化，潜移默化地影响着受众的感受和价值判断。文化是一个民族凝聚力的重要因素，这种利用网络实施的“文化侵略”是极其危险的，危及民族文化的独立与自存，甚至有可能动摇民族、国家的根基。对此，我们必须有充分的认识和积极的准备，必须慨然担当起继承和弘扬民族优秀传统文化的重任，确保中国文化安全。

1.2.3　研究项目和网络安全基础设施

在国内，信息系统安全方面的建设可以追溯到“七五”与“八五”期间，我国在信息加密、解密、密钥芯片、密钥管理等方面有所研究，到了 20 世纪 90 年代，在信息安全的传统思路上，科学院成立了信息安全技术工程研究中心，主要从事上述技术中加密与解密的研究工作。但是，所有这些主要停留在传统的信息安全的概念上，对系统的安全重视不够。信息产业部 15 所（太极计算机公司）在“九五”期间进行 UNIX 操作系统的安全研究工作，于 1998 年验收和鉴定了自主开发的 UNIX 操作系统 B1 级安全核开发工作。同时在太极联合实验室，启动了与国际水平接轨的网络和系统的安全测试、管理和监控软件的自主开发。太极计算机公司研制成功了自主开发系列服务器产品、ATM 网络接人交换设备、1 000 兆以太网络、100 兆自适应网络接口设备、安全路由器以及分布式防火墙。这些产品已经应用于政府要害单位的系统中。

另外，中国软件与服务总公司在“八五”期间开发了具有自主版权的 UNIX 操作系

统。在北京信息工程学院、东大软件园区、人民大学信息学院等单位开发了自主版权的数据库管理系统。由解放军信息工程大学信息工程学院研制的新一代高性能核心路由器系统，2004 年 12 月 26 日通过国家鉴定和验收。整机交换网络容量 3 200 亿比特，国内领先；转发速率每秒 2 亿次，国内第一；核心芯片，全部实现国产化。整体技术居国内领先、世界先进水平，对国家信息网络安全具有重大意义。这种新一代核心路由器还具有极大的军用价值。首先，该路由器全部采用国产芯片，把住了我国信息安全的命脉；其二，该机采用全分布式体系结构，具有极强的抗打击能力。主控系统若遭破坏，其任意一个从属交换系统便可在短时间内迅速升级，承担起主交换系统的功能，确保网络畅通无阻。核心路由器的研制还为信息化提速和向宽带化进军提供了技术、产品和经验支持。

随着国际政治形势的发展，以及经济全球化过程的加快，人们越来越清楚，信息时代所引发的信息安全问题不仅涉及国家的经济安全、金融安全，同时也涉及国家的国防安全、政治安全和文化安全。因此可以说，在信息化社会里，没有信息安全的保障，国家就没有安全的屏障。信息安全的重要性怎么强调也不过分。信息安全领域的对抗，很大程度上是技术与技术的较量。要从根本上解决国家和军队的信息安全问题，必须发扬“两弹一星”精神，来研制我们中国人自己的 CPU、操作系统、网络方案、密码芯片和大型数据库等。

进入新世纪以来，我国自主研制的半导体芯片、操作系统、网络路由器等相继取得了进展，我国自主研制信息系统的工作已经起步。但是，我们的技术研发工作还比较分散，没有完全形成合力；经费投入不足，技术和产品还没有形成体系。要构筑起一套可靠的信息安全体系，还需要举全国之力。当务之急，是吸引和培养一批一流的信息技术人才。

第2章

信息安全的基本要素

2.1 网络与信息安全的概念

2.1.1 网络信息安全的定义

国际标准化组织（ISO）对计算机信息系统安全性的定义为：“为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。”计算机信息系统安全包括物理安全和逻辑安全，其中物理安全指系统设备及相关设施的物理保护以免于被破坏和丢失。逻辑安全是指信息的可用性、信息的完整性和信息的机密性。计算机信息系统的安全就是本章要讨论的网络信息系统安全，简单地表述为信息安全。

2.1.2 网络信息安全问题研究

谈到信息安全，我们不得不面临一些极为重要的问题，这些问题是任何希望设置一种有效的安全机制的人必须回答的。首要问题是：“我们力图保护的是些什么资源？”答案并不总是明确的。是 CPU 周期吗？在一定时期内，这个问题很有意义，因为那时计算机时间非常昂贵。但如今这已不再是问题了，当然超级计算机是一个例外。与 CPU 周期相比，更为严重的是 CPU，或者更确切地说，运行按一定配置文件定制的特定软件的 CPU 的名字或标识，这使它可以访问其他更重要的资源。这些通常比 CPU 时间更敏感。一个打算破坏或模仿一台主机的黑客通常将对该主机全部资源进行访问：文件、存储设备、电话线等。通过实际的分析发现，某些黑客最感兴趣的是滥用主机标识，而不是过分触及主机的专门资源，他们利用这些标识，暗渡陈仓，向外连接他们更感兴趣的目标。当然，人们通常想保护所有资源，在这种情况下，最明显的答案是把攻击者拒之门外，即首先不让他们进入计算机系统。这样的方法是一个有用的开端，虽然，它假设系统安全问题来自外部。

第二个主要问题：“计算机系统必须防范谁？”那些足以对付一个使用调制解调器的年轻人的技术，在重要的情报部门面前却无能为力。对于前者，增强口令安全性即可解决问题，然面后者却能够、并且可能借助于搭线窃听和密码分析，监视你的计算机和电缆的电子发射，甚至瞄准你在计算机房的“暗箱操作”。计算机安全并不是目的，它

是达到信息安全这一目的的手段。如果必要和合适的话，还应该采用其他手段。计算机安全防范的强度与其所受的威胁成比例。假如有 200 万主机登录，那么有多少人访问这些计算机呢？又有多少人试图在这些机器上一试黑客身手，甚至以黑客为职业呢？

在配置安全机制之前必须回答的第三个问题："你能在安全方面付出多大代价？"安全问题的部分代价是直接的财政开支，诸如建立防火墙网关需要额外的路由器和计算机。通常，容易忽视设置和运行网关的管理费用。而且还有一些更微妙的开支——方便性、生产性，甚至道德问题引起的开支。过分的安全性可能像过低的安全性一样有害。找出适当的安全性平衡点是棘手的、却又是完全必要的。并且，只有当你从两个极端对你的组织机构的安全风险进行了恰当评估后才可能做到这一点。安全即寻求平衡。

2.1.3 网络安全和信息安全基本要素

一、网络中存在的问题主要包括以下几个方面

一是无主管的自由王国（有害信息、非法联络、违规行为）。

二是不设防的网络空间（国家安全、企业利益、个人隐私）。

三是法律约束脆弱（黑客犯罪、知识侵权、逃避税收）。

四是跨国协调困难（过境信息控制、跨国黑客打击、关税）。

五是民族化和国际化的冲突（文化传统、价值观、语言文字）。

六是网络资源紧缺（IP 地址、域名、带宽）。

二、网络安全涉及的因素

1. 关于物理安全

作用点：对计算机网络与计算机系统的物理装备的威胁，主要表现在自然灾害、电磁辐射与恶劣工作环境方面。

外显行为：通信干扰，危害信息注入，信号辐射，信号替换，恶劣操作环境。

防范措施：抗干扰系统，防辐射系统，隐身系统，加固系统，数据备份。

2. 关于系统安全

作用点：对计算机网络与计算机系统可用性与可控性进行攻击。

外显行为：网络被阻塞，黑客行为，非法使用资源等，计算机病毒，使得依赖于信息系统的管理或控制体系陷于瘫痪。

防范措施：防止人侵，检测人侵，攻击反应，系统恢复。

3. 关于信息安全

作用点：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。

外显行为：窃取信息，篡改信息，冒充信息，信息抵赖。

防范措施：加密，完整性技术，认证，数字签名。

4. 政治文化安全

作用点：有害信息的传播对我国的政治制度及传统文化的威胁，主要表现在舆论宣传方面。

外显行为：淫秽暴力信息泛滥、敌对的意识形态信息涌人、英语文化的"泛洪现象"对民族文化的冲击，网络被利用作为串联工具，传播迅速，影响范围广。