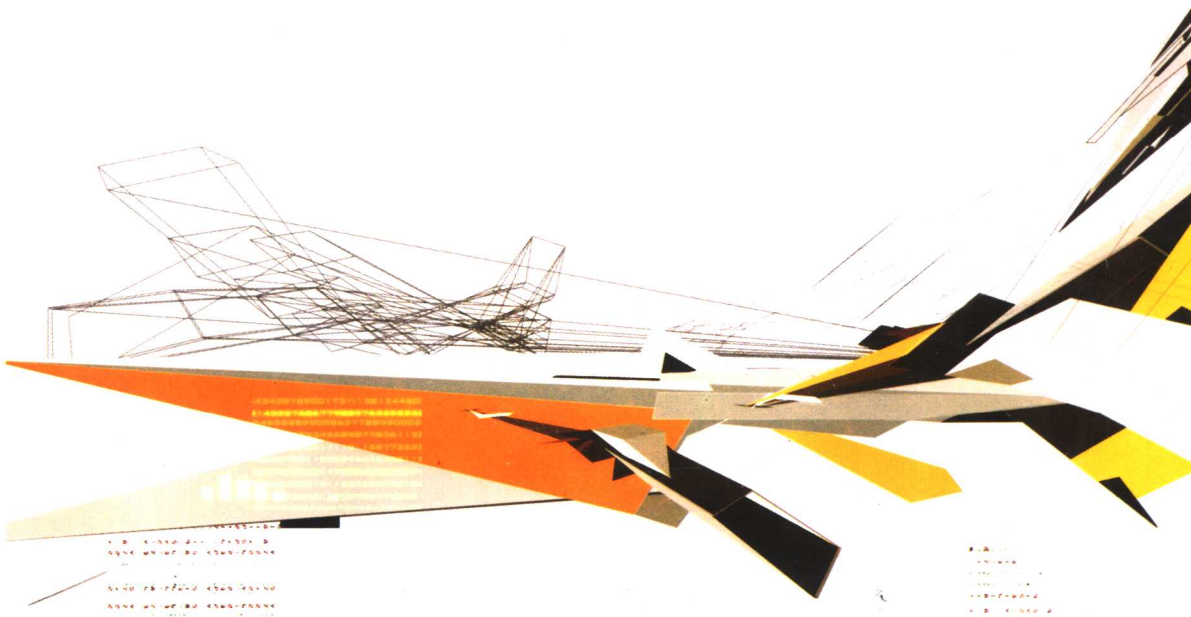
W L X X A Q Y L H Y Y

公务员
专业技术人员
培训教材

网络信息安全

原理和应用

主编/ 沈敦厚



海南出版社

公　务　员
专业技术人员培训教材

网络信息安全原理和应用

主　　编：沈敦厚

执行编委：谢永志　钟文平　刘　栋
　　王作为　周宏强　林济银

海南出版社

图书在版编目(CIP)数据
网络信息安全原理和应用 / 沈敦厚编. -海口：海南出版社，2006.6
ISBN 7-5443-1729-3
Ⅰ.网…… Ⅱ.谢…… 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（2006）第063463号

网络信息安全原理和应用
主　　编:沈敦厚
责任编辑:古　华
海南出版社　出版发行
地　　址:海口市金盘开发区建设三横路2号
邮　　编:570216
电　　话:0731—4918670
印　　刷:湖南省书报刊发行业协会湘联印刷厂
出版日期:2006年6月第1版　2006年6月第1次印刷
开　　本:787×1092　1/16
印　　张:12.5
印　　数:1-5100册
书　　号:ISBN7-5443-1729-3/TP•33
定　　价:20.00元

前 言

随着世界信息化的发展，计算机网络及信息化系统在政府机构、企事业单位及社会团体的运作中发挥着越来越重要的作用。信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统本身的脆弱性和日益呈现的复杂性，信息安全问题不断暴露。信息安全既关系着个人、单位的隐私，也关系着国民生计，乃至整个国家的安全与利益。信息安全问题已经备受政府和社会的广泛关注和重视。2004 年国家召开信息安全保障体系建设的会议，标志着我国信息安全保障体系建设的开始。自此，我国政府大力推行信息化工程，连续推出电子商务年、电子政务年并提出了信息系统等级保护管理办法，这些都说明我国政府已经将信息安全提到了国家安全的高度。在这样的背景下，国家对信息安全从业人员的安全意识、安全技能提出了相关要求。本教材正是基于此种需求而编写的。

本教材充分考虑了信息安全从业人员的需要，以信息安全从业人员所应具备的知识体系为大纲，从互联网的概念、发展历程、互联网的特点及信息安全的理论基础出发，兼顾理论学习与实践应用，较全面地覆盖了信息安全体系的知识要点。本教材内容涉及到网络信息安全意识、网络信息安全现状、信息安全保障体系、密码技术、网络安全、系统安全、风险评估、安全策略、安全工程、信息安全管理、应急响应、国内外相关标准及法律法规等诸多方面，能帮助相关人员对信息安全学科有一个较为全面的了解。

网络信息安全不仅是信息安全专业技术问题，更是管理的问题。本书作为引玉之砖，期望有更多的人能够关注信息安全并参与到其中来。

周红军

2006 年 5 月 18 日

目 录

第 1 章　互联网(Internet)的发展和特性

无论从技术还是从经济角度看，Internet 的出现都是人类进步的巨大成就。到目前为止，Internet 仍然处在其发展的早期阶段，Internet 的商业应用截至 2006 年在国内不到 20 年的时间，在很多领域的发展还未成熟，因此，现在对 Internet 的影响做出全面评价还为时过早。Internet 对经济、技术与人类生活的影响将随着 Internet 的普及与应用而逐渐体现出来。

在这样一个时期，如何利用与发展 Internet，使其为人类造福，已成为各国政策的重要内容。从其技术特征与发展历程看，Internet 是一个分布式、非控制性、虚拟的网络，在网络上的所有结点都是平等的。没有一个国家的政府、机构能够完全控制 Internet，但这并不意味着 Internet 完全不可控。世界各国的政府与学术界都在讨论 Internet 的管理问题，即使是在美国，也有许多机构甚至地方政府都主张对 Internet 进行管制。但从实际结果看，Internet 仍然是不受管制的。在美国，对 Internet 采取非管制政策有两个原因：（1）Internet 仍然处于发展的早期，仍然需要大量资金投资于 Internet 的网络与创新，只有一个自由的、不受管制的环境才能够最大限度地刺激这些投资；（2）没有一个管制机构享有对 Internet 进行全面管制的法律授权。Internet 涉及很多方面，任何一个管制机构都没有相应的法律对 Internet 进行全面的管制。如根据通信法授权，联邦通信委员会有管制公共电信公司的权力，但是，Internet 服务提供商不属于公共电信公司，因此，联邦通信委员会不能对其运用通信法的有关条款进行管制。同理，Internet 服务商也不是 CABLE 公司，不是广播公司、出版公司，因此，也不能沿用相应的法律来管制。截至现在，从宏观上考察，Internet 是不受管制的。

Internet 不受管制并不是说 Internet 没有管理问题。在本章将讨论与 Internet 的管理有关的问题，重点介绍涉及公共电信公司提供 Internet 服务的管制问题。

1　Internet 的概念

1.1　Internet 是什么

由于 Internet 涉及的领域很多，因此，很难给出明确定义。从技术角度看，人们会将 Internet 理解为以 TCP/IP 为代表的一系列协议。从网络角度看，人们会认为它是网络的网络。从新闻传播的角度看，它是一种新型传播介质。从经济角度看，它代表一个新兴的产业群。Internet 处于高速的发展之中，其技术与应用远未定型，所以许多新的技术与应用领域不断出现，在这样的形势下要给出 Internet 的严格定义几乎是不可能。尽管有这样或那样的困难，人们还是在努力尝试给出 Internet 的定义。1995 年 10 月 34 日，美国联邦网络理事会给出了一个定义 Internet 的办法，并以此向 Internet 业内人士和知识产权界人士征求意见。我们不妨借用一下这个定义以说明问题。

Internet 是指一个全球化的信息系统，这个系统：

1. 建立在 IP 及其扩展协议基础上，通过全球唯一的空间地址进行逻辑连接。

2. 能够支持使用 TCP/IP 协议及其扩展协议与兼容协议的传输。

3. 能够向公众或个人提供使用或接入其与上述通信与基础设施上的高层次的服务。

为了更好地说明 Internet，我们将 Internet 的技术特点作一个简单介绍，以此作为对 Internet 定义的补充。

1.2 Internet 的产生与发展

1.2.1 早期的 Internet

早期的 Internet 始于 1969 年，为适应冷战时期的需要，美国国防部高级项目研究署资助开发一种通信网络，通过这一网络，系统上的任何一点，可以与系统上的其他各点进行有效的通信联络，任何一个结点发生故障都只影响该结点与其他结点的通信而不会影响到其他结点间的通信，这就是 ARPANET。通过这一网络，美国国防部将所属军事机构、国防合同单位和从事与国防项目有关的大学与研究机构的计算机连接在一起。这是一个只有 64K 带宽和 4 个结点的通信网络，但是，在网络发展过程中起到了开拓性的示范作用。

1970 年和 1971 年，ARPANET 的结点数分别为 9 个和 15 个，到 1972 年，结点数达到 37 个。也就是在这一年，电子邮件产生了。1973 年，TCP 协议的第一稿产生。它的两项关键功能是：流量控制和查错，大大提高了网络的可靠性。1975 年 7 月，由于 ARPANET 上与军事有关的业务流量越来越大，美国国防部高级项目研究署将 ARPANET 转交给国防部通信署。由于接入 ARPANET 受到限制，导致了其他计算机网络的发展。1978 年，IP 协议产生，IP 提供了给寻址所需要的所有信息并实现基本的分组交换功能。自此，TCP/IP 协议组产生。

在 20 世纪 70 年代和 80 年代，其他一些机构也纷纷仿效美国国防部，建设许多类似的通信网。这个时期建设的计算机通信网有：美国能源部建设的 MFENET，美国国家宇航局建设的 SPAN 网络，3COM 公司建设的 UNET，受到美国国家科学基金会资助的 CSNET，它们将不能联入 ARPANET 的研究机构联接在一起。所有这些网络都是相对独立的，使用各自不同的技术规范。但其中很大一部分网络采用的是 TCP/IP 协议组。1982 年，APRA 决定将 ARPANET 上采用的 NCP 协议全部转换成 TCP/IP 协议，转换工作于 1983 年 1 月 1 日前完成，这标志着 Internet 的真正诞生。同年，国防部通信署将 ARPANET 分解成两个部分，与军事有关的通信任务逐渐转移给国防数据网(Defense Data Network)，与研究相关的通信业务继续留在 ARPANET 并与 CSNET 联通。

1985 年，美国国家科学基金会开始投资建设 NSFNET，将分别设在普林斯顿大学、彼兹堡大学、加州大学圣地亚哥分校、伊利诺斯大学和康奈尔大学的 5 个超级计算中心连接起来。这个网络最初的带宽只有 64K，除了联接上述超级计算中心外，还允许其他一些地区性计算机网络和没有超级计算机的大学网联入，构成了一个联接各大学的计算机网络。与此同时，美国国家科学基金会强制要求将 TCP/IP 协议作为 NSFNET 的协议标准。成为第一个实际上的 IP 骨干网。作为 NSFNET 的一部分，8 个地区性计算机网建成，并联入了 NSFNET。所有接受美国国家科学基金资助的大学都可以联入 NSFNET，而且联入的条件是“必须让校园内所有符合条件的用户都能够接入网络”。

到 1986 年时，这个网络基本上由 3 个层次组成：

1. 本地网，将一个校园内的计算机资源连接起来的局域网。

2. 地区网，将同一地区内的计算机校园网连接起来组成的网络。

3. 骨干网，将地区网连接起来并负责地区网之间的信息交流的全国性网络。

1.2.2　20 世纪 90 年代 Internet 的商业化

20 世纪 90 年代，商业机构介入 Internet，带来 Internet 的第二次飞跃。

至 Internet 问世后，每年加入 Internet 的计算机成指数式增长。NSFNET 在完成的同时就出现了网络负荷过重的问题。意识到美国政府无力承担组建一个新的更大容量的网络的全部费用，NSF 鼓励 MERIT、MCI 与 IBM 三家商业公司接管了 NSFNET。

三家公司组建了一个非盈利性的公司 ANS，并在 1990 年接管了 NSFNET。到 1991 年底，NSFNET 的全部主干网都与 ANS 提供的新的主干网连通，构成了 ANSNET。与此同时，很多的商业机构也开始运行它们的商业网络并连接到主干网上。

Internet 的商业化，开拓了其在通信、资料检索、客户服务等方面的巨大潜力，导致了 Internet 新的飞跃，并最终走向全球。

从 INTERNET 的发展过程可以看到，Internet 是历史的沿革造成的，是千万个可单独运作的子网以 TCP/IP 协议互联起来形成的，各个子网属于不同的组织或机构，而整个 Internet 不属于任何国家、政府或机构。

1.2.3　全面应用阶段

Internet 发展至今，已经与人们的工作、生活息息相关、密不可分，已经逐渐地改变了人们的交流方式、生活方式；改变了全球的经济结构、社会结构；使整个人类社会成为一个地球村。Internet 越来越成为人类社会的一个重要的组成部分，尤其是与各种大型、关键业务系统的结合越来越紧密，如党政部门信息系统、金融业务系统、企业商务系统等。Internet 已经融入了政治、金融、文化、生活等领域。基于 Internet 的应用也日益丰富。总之，Internet 的发展日新月异，给人们的工作生活带来了极大的便利，已经成为了现代生活不可或缺的一部分。

图 1.1 为一个典型的网络应用图。

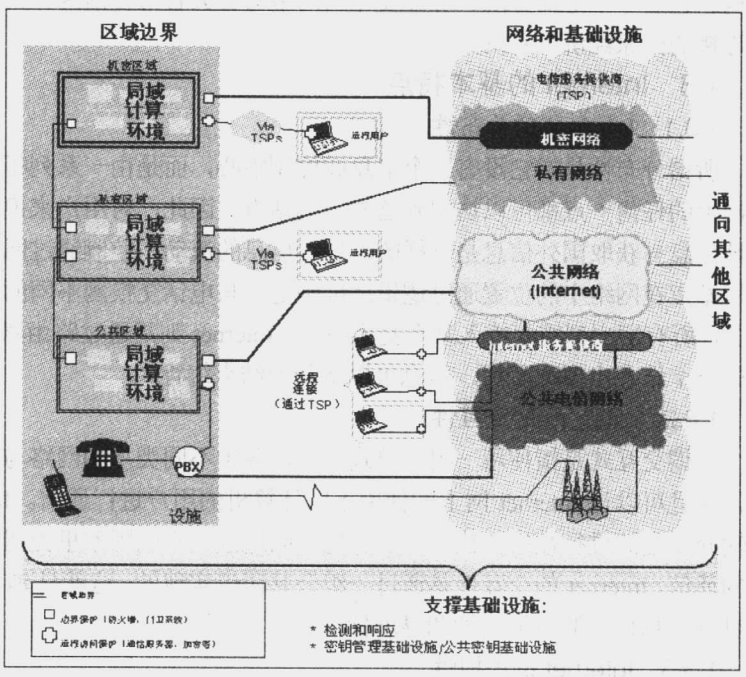


图 1.1　一个典型的网络应用图

1.2.4 我国的 Internet 发展

Internet 在我国的发展经历了两个阶段：第一阶段是 1987 年至 1993 年，这一阶段实际上只是少数高等院校、研究机构提供了 Internet 的电子邮件服务，还谈不上真正的 Internet；第二阶段从 1994 年开始，实现了和 Internet 的 TCP/IP 连接，从而开通了 Internet 的全功能服务。

根据国务院的规定，有权直接与国际 Internet 连接的网络有 4 个：中国科技网 CSTNet、中国教育科研网 CERNET、中国公用计算机互联网 ChinaNet、中国金桥信息网 CHINAGBN。

中国科技网(China Science and Technology Network ，简称 CSTNet)。包括中国科学院北京地区已经入网的 30 多个研究所和全国 24 个城市的各学术机构，并连接了中国科学院以外的一批科研院所和科技单位，是一个面向科技用户、科技管理部门及与科技有关的政府部门的全国性网络。

中国教育科研网(China Education and Research Network，简称 CERNET)。这是一个全国性的教育科研计算机网络，把全国大部分高等学校和中学连接起来，推动学校校园网的建设和信息资源的交流共享，从而极大地改善我国大学教育和科研的基础环境，推动我国教育和科研事业的发展。CERNET 网络由三级组成：主干网、地区网、校园网。其网控中心设在清华大学。地区网络中心分别设在北京、上海、南京、西安、广州、武汉、沈阳、成都。

中国公用计算机互联网(简称 ChinaNet)是由原邮电部建设的，主要用于民用和商用。该网络目前已覆盖了全国 31 个省市。

中国金桥信息网(China Golden Bridge Network，简称 CHINAGBN)由原电子工业部归口管理，是以卫星综合数字业务网为基础，以光纤、微波、无线移动等方式形成天地一体的网络结构。它是一个把国务院、各部委专用网络与各大省市自治区、大中型企业以及国家重点工程连接的国家经济信息网。

1.3 Internet 的基本特点

1.3.1 Internet 的分布性

所谓分布性是指它没有一个信息或控制中心，而是由一系列相互联接的主机站点组成，从网上的任何一点都可以访问到这些主机站点。因此，对用户来说，在 Internet 网上，获取本地信息与获取国外信息是一样的。这些信息的流动与控制通过网络结构的层次进行。每个主机站点在网络中的位置通过逻辑地址确定。与电话交换网不同的是，电话交换网是中央控制的，所有用户都需要接入某个交换中心。Internet 则是通过路由器管理信息的交换，当网络上的一个结点出现故障后，信息可以从其他结点绕行。

1.3.2 Internet 的交互性

所谓交互式是指使用一组开放式协议，各种不同类型的网络与设施可以透明地连接在一起，并且可以让 Internet 网上的使用不同计算机的用户进行通信。Internet 可以在各种不同的传输介质之间进行数据传输，可以实现不同地区、不同国家里使用不同类型计算机的用户之间的通信。Internet 的交互性是通过一组公共协议实现的，这就是 TCP/IP，它定义了在 Internet 上进行信息传输的数据结构和寻址标准。

1.3.3 Internet 的虚拟性

所谓虚拟性是指对于连接到 Internet 的用户，你无法判断对方的身份信息的真实性，如

姓名、性别、年龄、IP 地址等信息，Internet 的虚拟性很好地隐藏了个人隐私，但是同时也为网络诈骗提供了可乘之机，增加了网络犯罪调查取证的难度。

1.3.4　Internet 的平面性

Internet 的所有结点都是平等的，呈平面结构，没有高低贵贱之分，也没有上下级的区分，在 Internet 上人人平等，享有最大限度的言论自由，但是也给 Internet 的管理带来了极大的不便。

1.3.5　Internet 的开放性

Internet 是一个很好的资源共享的平台，网上的用户可以很容易地发表自己的言论和相关资料，网上的任何用户也很容易浏览到一个企业、单位，以及个人的敏感性信息。受害用户甚至连自己的敏感性信息被别人盗用了却全然不知。

1.3.6　Internet 的信息资源的高度聚集性

通过 Internet 可以收集各方各面的资料，当信息分离的小块出现时，信息的价值往往不大。但是将大量相关信息聚集在一起时，却可以显示出其重要价值。

网络自身的这些特点，在为各国带来发展机遇的同时也必将带来巨大的风险。随着网络经济和网络时代的发展，网络已经成为一个无处不有、无所不用的工具。经济、文化、军事和社会活动将会强烈地依赖于网络，而网络信息安全业已成为世界各国共同关注的焦点。

2　网络信息安全概念和认识

应该说 Internet 是一把双刃剑，它为我国国民经济建设、人们的物质文化生活带来促进和丰富的同时，也对传统的国家安全体系提出了严峻的挑战，使得国家机密、金融信息等面临着巨大的安全威胁。Internet 的最大特点就是开放性，但对于安全来说，这又是它致命的弱点。但是，正确的态度应该是辩证的，一方面不能因噎废食，拒绝先进的网络技术和文化，另一方面一定要对网络信息安全给予充分的重视。

网络信息安全是一个关系国家安全和主权、社会稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变得越来越重要。“家门就是国门”，安全问题刻不容缓。

网络信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络信息安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络信息安全从本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络信息安全的具体含义会随着“角度”的变化而变化。如从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和

控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

本节首先将国内对信息安全概念的各种理解归纳为两种描述，一种是对信息安全所涉及层面的描述；一种是对信息安全所涉及的安全属性的描述。然后提出了以经纬线的方式将两种描述风格融为一体的方法，即基于层次型描述方式。同时，在传统的实体安全、运行安全、数据安全三个层面的基础之上，扩充了内容安全层面与信息对抗层面，并将其归类为信息系统、信息、信息利用三个层次。另外还针对国外流行的信息安全金三角的描述，扩充为信息安全四要素，从而完备了对信息安全概念框架的描述。最后，给出了关于信息安全的定义。

2.1 背景

“信息安全”曾经仅是学术界所关心的术语，就像是 20 世纪五六十年前“计算机”被称为“电算机”那样仅被学术界所了解一样。现在，“信息安全”因各种原因已经像公众词汇那样被广大公众所熟知，尽管尚不能与“计算机”这个词汇的知名度所比拟，但也已经具有广泛的普及性。问题的关键在于人们对“计算机”的理解不会有什么太大的偏差，而对“信息安全”的理解则往往各式各样。种种偏差主要来自于从不同的角度来看信息安全，因此出现了“计算机安全”、“网络安全”、“信息内容安全”之类的提法，也出现了“机密性”、“真实性”、“完整性”、“可用性”、“不可否认性”等描述方式。

通俗地说，安全就如图 1.2 所示：

图 1.2 打不跨

关于信息安全的定义，以下收集一些有代表性的定义方式：

国内学者给出的定义是：“信息安全保密内容分为：实体安全、运行安全、数据安全和管理安全四个方面。”

我国计算机信息系统安全专用产品分类原则给出的定义是：“涉及实体安全、 运行安全和信息安全三个方面。”

我国相关立法给出的定义是：“保障计算机及其相关的和配套的设备、设施（网络）的安全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全”。这里面涉及了物理安全、运行安全与信息安全三个层面。

国家信息安全重点实验室给出的定义是：“信息安全涉及到信息的机密性、完整性、可

用性、可控性。综合起来说，就是要保障电子信息的有效性。”

英国 BS7799 信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”

美国国家安全局信息保障主任给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部我们用‘信息保障’来描述信息安全，也叫‘IA’。它包含 5 种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。”

国际标准化委员会给出的定义是：“为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露”。这里面既包含了层面的概念，其中计算机硬件可以看作是物理层面，软件可以看作是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

纵观从不同的角度对信息安全的不同描述，可以看出两种描述风格。一种是从信息安全所涉及层面的角度进行描述，大体上涉及了实体（物理）安全、运行安全、数据（信息）安全；一种是从信息安全所涉及的安全属性的角度进行描述，大体上涉及了机密性、完整性、可用性。

2.2　信息安全多种理解的缘由

信息安全出现多种不同说法，存在着多种观察视角，并不是偶然的现象。从信息安全的发展历史、信息安全的作用层面、信息安全的基本属性，都决定了信息安全的不同内涵。

从信息安全的发展历史来看，早在 20 世纪四五十年代，人们认为信息安全就是通信保密，采用的保障措施就是加密和基于计算机规则的访问控制，这个时期被称为“通信保密（COMSEC）”时代，其时代标志是 1949 年 Shannon 发表的《保密通信的信息理论》；在 70 年代，人们关心的是计算机系统不被他人所非授权使用，这时学术界称之为“计算机安全（INFOSEC）”时代，其时代特色是美国 20 世纪 80 年代初发布的橘皮书——可信计算机评估准则（TCSEC）；90 年代，人们关心的是如何防止通过网络对联网计算机进行攻击，这时学术界称之为“网络安全（NETSEC）”，其时代特征是美国 80 年代末出现的“莫里斯”蠕虫事件；进入了 21 世纪，人们关心的是信息及信息系统的保障，如何建立完整的保障体系，以便保障信息及信息系统的正常运行，这时学术界称之为“信息保障（IA）”。

从信息安全的作用层面来看，人们首先关心的是计算机与网络的设备硬件自身的安全，就是信息系统硬件的稳定性运行状态，因而称之为“物理安全”；其次人们关心的是计算机与网络设备运行过程中的系统安全，就是信息系统软件的稳定性运行状态，因而称之为“运行安全”；当讨论信息自身的安全问题时，涉及的就是狭义的“信息安全”问题，包括对信息系统中所加工存储、网络中所传递的数据的泄漏、仿冒、篡改以及抵赖过程所涉及的安全问题，称之为“数据安全”。因此，就信息安全作用点来看问题，可以称之为信息安全的层次模型，这也是国内学者普遍认同的定义方式，如图 1.3 所示。

数据（信息）安全
运行（系统）安全
物理（实体）安全

图 1.3 一种信息安全的层次模型

从信息安全的基本属性来看，机密性就是对抗对手的被动攻击，保证信息不泄漏给未经授权的人，或者即便数据被截获，其所表达的信息也不被非授权者所理解。完整性就是对抗对手主动攻击，防止信息被未经授权的篡改。可用性就是确保信息及信息系统能够为授权使用者所正常使用。这三个重要的基本属性被国外学者称为信息安全金三角（CIA），如图 1.4 所示。

2.3 信息安全概念经纬线

从信息安全的作用层次来看，前面已经介绍了人们所关注的三个层面，即物理安全层、运行安全层及数据安全层。但是，还有两个层面尚没有人在同一个框架之下给出清晰的描述。一个是关于信息内容的安全问题，一个是关于信息对抗的问题，而这两个层面的安全问题也是业界普遍关心的问题。所不同的是，内容安全更被文化、宣传界人士所关注；而信息对抗则更被电子对抗研究领域的人士所关注。

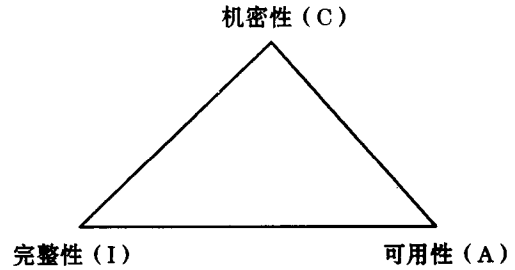


图 1.4 信息安全金三角模型

信息内容安全的问题已经深刻地展现在现实社会的面前，主要表现在有害信息利用互联网所提供的自由流动的环境肆意扩散，其信息内容或者像脚本病毒那样给接收的信息系统带来破坏性的后果，或者像垃圾邮件那样给人们带来烦恼，或者像谣言那样给社会大众带来困惑，从而成为造成社会不稳定的因素。但是，就技术层面而言，信息内容安全技术的表现形式是对信息流动的选择控制能力，换句话说，表现出来的是对数据流动的攻击特性。

信息对抗严格上说是信息谋略范畴的内容，是讨论如何从多个角度或侧面来获得信息并分析信息，或者在信息无法隐藏的前提下，通过增加更多的无用信息来扰乱获取者的视线，以掩藏真实信息所反映的含义。从本质上来看，信息对抗是在信息熵的保护或打击层面上讨论问题，也就是围绕着信息的利用来进行对抗。信息熵是指从随机试验的角度对客观事物进行分析，并在结果分析过程中的不确定性。

从信息安全的属性来看，除了前面所介绍的机密性、完整性、可用性等三个基本属性之外，还有更多的一些属性也用于描述信息安全的不同的特性，如真实性、可控性、合法性、实用性、占有性、唯一性、不可否认性、可追溯性、生存性、稳定性、可靠性、特殊性等。其中：真实性反映的是主体身份、行为及相关信息的真实有效；可控性反映的是信息系统不会被非授权使用，信息的流动可以被选择性阻断；合法性反映的是信息或信息系统的行为获得了授权；实用性反映的是信息加密密钥与信息的强关联性及密钥不可丢失的特性；占有性反映的是信息载体不可被盗用，确保由合法信息所占有；唯一性反映的是各信息以及信息系