网络与信息安全基础

—— 本书编委会编著 ——

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

网络与信息安全基础

本书编委会编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内容简介

信息安全是一个综合的交叉学科，涉及计算机、通信、信息、法律、管理等许多学科，内容广泛。本书从信息安全基础理论入手，通过对常见的网络攻击和检测技术、信息保护技术、网络防火墙、容灾和数据备份技术、应急响应和灾难恢复技术、网络应用安全问题、系统安全应用以及互联网信息内容安全管理和互联网上网服务营业场所管理等方面的阐述，使读者能在信息安全技术和技能方面有所认识和了解。

图书在版编目(CIP)数据

网络与信息安全基础/《网络与信息安全基础》编委会编著. —北京：北京理工大学出版社，2008.3

ISBN 978-7-5640-1462-9

Ⅰ.网…　Ⅱ.网…　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(2008)第 035064 号

出版发行/北京理工大学出版社

社　　址 / 北京市海淀区中关村南大街 5 号

邮　　编 / 100081

电　　话 / (010)68914775(办公室)　68944990(批销中心)　68911084(读者服务部)

网　　址 / http://www.bitpress.com.cn

经　　销 / 全国各地新华书店

印　　刷 / 北京市通县华龙印刷厂

开　　本 / 787 毫米×1092 毫米　1/16

印　　张 / 33.25

字　　数 / 800 千字

版　　次 / 2008 年 3 月第 1 版　　2008 年 3 月第 1 次印刷

定　　价 / 45.00 元

责任校对 / 陈玉梅

责任印刷 / 周瑞红

网络与信息安全基础

编 委 会

目 录

第一章　信息安全基础

第一节　信息安全基础知识

一、信息安全的概念

20世纪，人类在科学技术领域内最大的成就是发明制造了电子计算机。为了不断提高其性能，增加计算机的功能和应用范围，全球科学家和技术人员一直在孜孜不倦地进行试验和改进。在计算机更新换代的改进过程中，电子化技术、数字技术、通信技术以及网络技术不断融合和被广泛应用，从而使得以计算机为负载主体的互联网技术得以突破时空限制而普及全球，并由此开创了一个以电子信息交流为标志的信息化时代。随着科学技术特别是信息技术和网络技术的飞速发展以及我国信息化进程的不断推进，各种信息化系统已经成为国家的关键基础设施，它们支持着网络通信、电子商务、电子政务、电子金融、电子税务、网络教育以及公安、医疗、社会福利保障等各个方面的应用。相对于传统系统而言，数字化网络的特点使得这些信息系统的运作方式，在信息采集、储存、数据交换、数据处理、信息传送上都有着根本的区别。无论是在计算机上的储存、处理和应用，还是在通信网络上交换、传输，信息都可能被非法授权访问而导致泄密，被篡改破坏而导致不完整，被冒充替换而不被承认，更可能因为阻塞拦截而无法存取，这些都是网络信息安全上的致命弱点。因而，信息安全应运而生。

（一）信息的定义

要理解信息安全，首先要了解什么是信息。“信息”是当代使用频率很高的一个概念，也是很难说清楚的一个概念，目前比较流行的有以下几种说法：

（1）信息是用语言、文字、数字、符号、图像、声音、情景、表情、状态等方式传递的内容。

（2）1948年，信息论的奠基人之一，美国数学家申农（Shanon）第一个以信息公式的方式定义“信息是熵的减少”，这里用到的“熵”是不确定性的度量。申农的信息定义实际上是说，信息是“用来消除不确定的东西”。

（3）控制论的奠基人维纳（Wiener）在1948年指出：“信息就是信息，不是物质，也不是能量”。专门指出了信息是区别于物质与能量的第三类资源。

（4）有人说信息是事物表现的一般形式，信息就是消息，强调了信息的知识性。

（5）有人强调信息的作用性，发展申农的信息定义，提出信息是具有新内容与新知识的消息。

（6）有人则强调信息与通信的关系，并且进一步形成了三类看法：

①“技术信息”，认为信息是物质属性的反映，例如事物运动的状态与方式等。

②“语义信息”，认为信息是人们适应外部世界，并同外部进行内容交换的标记，例如各种知识与技能等。

③“价值信息”，认为信息是具有价值性、有效性、经济性及其他特性的知识，例如各种情报等。

据不完全统计，世界上有关信息的定义有 100 多种，它们都从不同的侧面、不同的层次揭示了信息的某些特征和性质，但至今仍没有统一的、能为各界普遍认同的定义。“信息”的定义之所以呈现多样化，主要有三方面的原因：第一，信息本身的复杂性，它是一个多元化、多层次、多功能的综合物；第二，信息科学是一门新兴学科，是一门“大”学科，它有许多分支学科，它的内涵与外延不很确切，而且随着社会、经济和科学技术的发展处于不断发展之中；第三，人们出于不同的研究目的或使用目的，从不同的角度或层次出发，对“信息”必然作出不同的理解与解释。

我国国家标准 GB4898—85《情报与文献工作词汇基本术语》中，关于“信息”的解释是：“Information，物质存在的一种方式、形态或运动状态，也是事物的一种普遍属性，一般指数据、消息中所包含的意义，可以使消息中所描述事件的不确定性减少”。这个定义首先明确了信息的本质是物质的属性，而不是物质实体本身。客观存在的一切事物，包括自然界、人体本身和人类社会，都是在不断运动着的，运动的物质，必然会产生相互作用和影响，从而引起物质结构、数量等多方面的变化，事物的这些变化，便成为信息产生的物质基础。因此，信息不是事物本身，而是由事物发出的数据、消息中所包含的意义。同时，这一定义明确了信息的认知知识的功能，即能减少不确定性的能力，可以说，信息是知识的源泉，知识是对获得信息进行处理并使之系统化的结果。这一功能是信息的基本功能，是人类解释客观世界发展规律的重要途径，知识的积累、科技的发展进步、经济文化的繁荣，都离不开信息的这一功能，经过大脑对信息的鉴别、筛选、归纳、提炼和存储，人类对客观世界的认识逐步深入，人类逐步进化、进步、发展。最后，这一定义明确了信息是指数据与消息中所包含的意义，是数据与消息这样的信息中所包含的内容，区分了信息与信息，从结构上使信息的概念更加准确。

一般意义上，信息(Information)是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。对现代社会来说，信息也是一种资产，包括计算机和网络中的数据，还包括专利、标准、商业机密、文件、图纸、管理规章、关键人员等，就像其他重要的商业资产那样，信息资产具有重要的价值，因而需要进行妥善保护。

(二)信息的性质和功能

信息具有下面一些重要的性质。

(1)普遍性：信息是事物运动的状态和状态变化的方式。因此，只要有事物的存在，只要事物在不断地运动，就会有它们运动的状态和状态变化的方式，也就存在着信息，所以信息是普遍存在的，信息具有普遍性。

(2)无限性：在整个宇宙时空中，信息是无限的，即使是在有限的空间中，信息也是无限的。一切事物运动的状态和方式都是信息，事物是无限多样的，事物的发展变化更是无限的，因而信息是无限的。

(3)相对性:对于同一个事物,不同的观察者所能获得的信息量可能不同。

(4)传递性:信息可以在时间上或在空间中从一点传递到另一点。

(5)变换性:信息是可变换的,它可以由不同载体用不同的方法来载荷。

(6)有序性:信息可以用来消除系统的不定性,增加系统的有序性。获得了信息,就可以消除认识主体对于事物运动状态和状态变化方式的不确定性。信息的这一性质使信息对人类具有特别重要的价值。

(7)动态性:信息具有动态性质,一切活的信息都随时间而变化,因此,信息也是有时效的。信息是事物运动的状态和状态变化的方式,事物本身在不断发展变化,因而信息也会随之变化。脱离了母体的信息因为不再能够反映母体的新的运动状态和状态变化方式,它的效用就会降低,以至完全失去效用,这就是信息的时效性。所以人们在获得信息之后,并不能就此满足,信息要及时发挥效用,要不断补充和更新。

(8)转化性:信息可以转化,在一定的条件下,信息可以转化为物质、能量。最主要的条件是信息必须被人们有效地利用。正确而有效地利用信息,就可能在同样的条件下创造更多的物质财富和能量。

上述这些性质是信息的主要性质。了解信息的性质,一方面有助于对信息概念进一步理解,另一方面也有助于人们更有效地掌握和利用信息。

信息的基本功能在于维持和强化世界的有序性,可以说,缺少物质的世界是空虚的世界,缺少能量的世界是死寂的世界,缺少信息的世界是混乱的世界。信息的社会功能则表现在维系社会的生存,促进人类文明的进步和人类自身的发展。信息的功能主要表现为:

信息是一切生物进化的导向资源。生物生存于自然环境之中,而外部自然环境经常发生变化,如果生物不能得到这些变化的信息,生物就不能及时采取必要的措施来适应环境的变化,就可能被变化了的环境所淘汰。

信息是知识的来源。知识是人类长期实践的结晶,知识一方面是人们认识世界的结果,另一方面又是人们改造世界的方法,信息具有知识的秉性,可以通过一定的归纳算法被加工成知识。

信息是决策的依据。决策就是选择,而选择意味着消除不确定性,意味着需要大量、准确、全面及时的信息。

信息是控制的灵魂。这是因为,控制是依据策略信息来干预和调节被控对象的运动状态和状态变化的方式;没有策略信息,控制系统便会不知所措。

信息是思维的材料。思维的材料只能是"事物的运动状态和状态变化的方式",而不可能是事物的本身。人的思维和智慧是信息过程的产物。

信息是管理的基础,是一切系统实现自组织的保证。

信息是一种重要的社会资源,虽然人类社会在漫长的进化过程中一直没有离开信息,但是只有到了信息时代的今天,人类对信息资源的认识、开发和利用才达到高度发展的水平。现代社会将信息、材料和能源看成支持社会发展的三大支柱,充分说明了信息在现代社会中的重要性。信息安全的任务是确保信息功能的正确实现。

(三)信息安全的定义

如果说信息是一家机构的资产,与其他资产一样,应受到保护,那么信息安全的作用

就是保护信息不受大范围威胁所干扰，使机构业务能够畅顺，减少损失及提供最大的投资回报和商机。信息及其支持进程、系统和网络是机构的重要资产。信息的保密性、完整性和可用性对机构保持竞争能力、现金流、利润、守法及商业形象至关重要。但机构及其信息系统和网络也越来越要面对来自四面八方的威胁，如计算机辅助的诈骗、间谍、破坏、火灾及水灾等。损失的来源如计算机病毒、计算机黑客及拒绝服务攻击等手段变得更普遍、大胆和复杂。信息安全就是要采取措施（相应的技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的危害降到最低程度，以此维护机构的正常运作。凡是涉及信息的保密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

安全（Security）并没有统一的定义，这里是指将信息面临的威胁降到（机构可以接受的）最低限度。同样，信息安全（Information Security）也没有公认和统一的定义。国内外对于信息安全的概念都比较含糊和笼统，但都强调的一点是：离开信息体系和具体的信息系统来谈论信息安全是没有意义的。因此人们通常从两个角度来对信息安全进行定义：一是从具体的信息技术系统来定义，二是从某一个特定信息体系（如金融信息系统、政务信息系统、商务信息系统等）的角度来定义。从学科和技术的角度来说，信息安全（学）是一门综合性学科，它研究、发展的范围很广，包括信息人员的安全性、信息管理的安全性、信息设施的安全性、信息本身的保密性、信息传输的完整性、信息的不可否认性、信息的可控性、信息的可用性等，确保信息系统按照预期运行且不做任何多余的事情，系统所提供的信息机密性可以得到适度的保护，系统、数据和软件的完整性得到维护和统一，以防任何可能影响任务完成的非计划的任务中断。长期以来，人们比较认同的关于信息安全的定义有两个：一个是美国联邦政府标准的定义——“保护信息系统免受意外或故意的非授权泄漏、传递、修改或破坏”；另外一个是我国信息安全国家重点实验室的定义——“信息安全涉及信息的保密性（Confidentiality）、可用性（Availability）、完整性（Integrity）和可控性（Controllability）。保密性就是保证信息不泄漏给未经授权的人；可用性就是保证信息以及信息系统确实为授权使用者所用；完整性就是抵抗对手的主动攻击，防止信息被篡改；可控性就是对信息以及信息系统实施安全监控。综合起来说，就是要保障电子信息的有效性”。国际标准化组织（ISO）定义信息安全为“为数据处理系统建立和采取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而遭到破坏、更改和显露”。随着计算机应用范围的逐渐扩大以及信息内涵的不断丰富，信息安全涉及的领域和内涵也越来越广。信息安全不仅是保证信息的机密性、完整性、可用性、可控性和可靠性，并且从主机的安全技术发展到网络体系结构的安全，从单一层次的安全发展到多层次的立体安全。目前，涉及的领域还包括黑客的攻防、网络安全管理、网络安全评估、网络犯罪取证等方面。因此在不会产生歧义时，常将计算机网络信息系统安全简称为信息安全。由于计算机网络具有联结形式多样性、终端发布不均匀性和网络开放性、互联性等特征，使得网络易受到黑客、恶意软件和其他不轨行为的攻击，所以网络信息的安全和保密性就是一个至关重要的问题。无论是在单机系统、局域网还是在广域网系统中，都存在着自然环境和人为等诸多因素的脆弱性和潜在威胁。因而计算机网络系统的安全措施应该是可以全方位地针对各种不同的威胁和脆弱性，才能确保网络信息的保密性、可用性、完

整性和可控性。一切影响计算机网络安全的因素和保障计算机网络安全的措施都是计算机网络安全的研究内容。在这里，我们可以这样来定义信息安全：信息安全是指信息在产生、传输、处理和储存过程中不被泄漏或破坏，确保信息的可用性、保密性、完整性和不可否认性，并保证信息系统的可靠性和可控性。

（四）信息安全的属性

信息安全的基本属性有信息的完整性、可用性、机密性、可控性、可靠性和不可否认性。

1. 完整性

完整性是指信息在存储、传输和提取的过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。一般通过访问控制阻止篡改行为，通过信息摘要算法来检验信息是否被篡改。完整性是数据未经授权不能进行改变的特性，其目的是保证信息系统上的数据处于一种完整和未损的状态。

2. 可用性

信息可用性指的是信息可被合法用户访问并能按要求顺序使用的特性，即在需要时就可取用所需的信息。可用性是信息资源服务功能和性能可靠性的度量，是对信息系统总体可靠性的要求。目前要保证系统和网络能提供正常的服务，除了备份和冗余配置外，没有特别有效的方法。

3. 机密性

信息机密性又称为信息保密性，是指信息不泄漏给非授权的个人和实体，或供其使用的特性。信息机密性针对信息被允许访问对象的多少而不同。所有人员都可以访问的信息为公用信息，需要限制访问的信息一般为敏感信息或秘密，秘密可以根据信息的重要性或保密要求分为不同的密级，如国家根据秘密泄露对国家经济、安全利益产生的影响（后果）不同，将国家秘密分为 A（秘密级）、B（机密级）和 C（绝密级）三个等级。秘密是不能泄漏给非授权用户、不被非法利用的，非授权用户就算得到信息也无法知晓信息的内容。机密性通常通过访问控制阻止非授权用户获得机密信息，通过加密技术阻止非授权用户获知信息内容。

4. 可控性

信息可控性是指可以控制授权范围内的信息流向以及行为方式，对信息的传播及内容具有控制能力。为保证可控性，通常通过握手协议和认证对用户进行身份鉴别，通过访问控制列表等方法来控制用户的访问方式，通过日志记录对用户的所有活动进行监控、查询和审计。

5. 可靠性

可靠性是指信息以用户认可的质量连续服务于用户的特性（包括信息的迅速、准确和连续地转移等），但也有人认为可靠性就是人们对信息系统而不是对信息本身的要求。

6. 不可否认性

不可否认性是指能保证用户无法在事后否认曾对信息进行的生成、签发、接收等行为，是针对通信各方面信息真实同一性的安全要求。一般用数字签名和公证机制来保证不可否认性。

（五）信息安全的特征

信息安全具有整体的、动态的、无边界和发展的特征，是一种非传统安全。信息安全涉及多个领域，是一个系统工程，需要全社会的共同努力和承担责任及义务；信息安全不是静态的，它是相对和动态的，经历了从最初纯粹的物理安全问题到今天随着信息技术的发展和普及，以及产业基础、用户认识、投入产出而出现的动态的全方位的安全问题；信息安全已经是全球性的而非某个国家或地区特有的问题，尤其是网络高度的互动性、渗透性使得信息安全问题变得越来越难以控制，不可避免地影响到我们生活的方方面面。信息安全是过程的安全，它不是固定不变的，而是贯穿于整个信息技术的发展过程中，应在系统建设过程中同步考虑。

互联网的全球性、快捷性、共享性、全天候性决定了信息安全问题的新特征。信息基础设施本身的脆弱性和攻击手段的不断更新，使信息安全领域易攻难守。网上攻击无论距离还是速度都突破了传统安全的限制，具有多维、多点、多次实施隐蔽打击的能力。由于网络覆盖全球，因而助长了犯罪分子的破坏能力和有恃无恐的犯罪心理，给世界带来了更多的不稳定因素。各国的民族文化和道德价值观面临前所未有的冲击和颠覆，为此付出的巨大经济成本和时间精力难以计算。信息安全问题日益严重必将给人类发展、国家管理和社会稳定带来巨大的危害。

信息安全属于非传统安全，非传统安全主要是相对于传统安全而言的。传统安全是指以军事安全为核心的安全；而将军事以外的对主权国家及人类整体生存与发展构成威胁的因素称为非传统安全。除军事以外的非传统安全问题主要包括：经济安全、金融安全、环境安全、信息安全、能源安全、恐怖主义、武器扩散、疾病蔓延、跨国犯罪等。由于冷战的结束，大规模军事对抗随着两极格局的消亡而退出主战场，非传统安全问题在我们今天的日常生活中正扮演着越来越重要的角色。在可预见的未来，由于经济全球化的大发展，世界越来越呈现出一种“你中有我，我中有你”的局面，取得“共赢”已逐渐代替“零和”（即我赢你输或我输你赢）的旧安全格局，大规模的军事对抗在可预见的未来发生的可能性很小，非传统安全将是未来我们将要长期面对的问题。

由于信息安全属于非传统安全，因此做好信息安全保障工作必须打破人们对国家安全观的固有认识。不能完全使用传统的办法来解决非传统的问题，需要综合运用政策、法律、管理、技术等手段。

二、信息安全的发展现状

从20世纪90年代末期开始，随着因特网的成熟和广泛应用，引发了一场全球范围内的信息革命，全球信息化的步伐不断加快，信息型社会正在形成并走向成熟。信息逐渐被作为一种重要的社会战略资源而与物质、能源、人才一起被列为现代社会生产力要素中的重要因素。信息化社会中，信息安全必然很重要。然而信息安全所面临的威胁也由来已久。自世界上出现计算机病毒理论后，对计算机系统的攻击就引起了一些人的兴趣。至今，这种攻击已由学术上的探讨，计算机操作系统的漏洞发现与弥补演变成了对信息系统的破坏和对涉及国家利益信息、商业信息及个人隐私信息的窃取和破坏。随着因特网的迅猛发展，更进一步暴露出了这种自由网络空间具有的无中心、无管理、不可控、不可信

等不安全的特征，且形成了对一切现存社会秩序的威胁。伴随着计算机网络的普及和广泛应用，导致信息安全泄密事件频频出现，计算机网络犯罪也呈现多样化的形式，网络欺诈、黑客入侵、计算机病毒、计算机破坏、信用卡犯罪等新问题层出不穷。因此，信息安全问题越来越受到各国政府部门和众多计算机专家、学者的广泛重视和研究，越来越多的研究机构开始对信息安全问题展开了探讨和研究。

（一）国内外发展和研究现状

从20世纪90年代开始，由于Internet技术广泛的应用，“黑客”活动日益猖獗，信息系统安全提出了许多新的问题，信息系统安全领域呼吁修改DoD585的橘皮书，美国颁布了新的联邦评测标准(FC)草案，用以代替80年代颁布的橘皮书。在上述标准的基础上，美国、加拿大和欧洲联合研制CC(信息技术安全评测公共标准)，并于1994年颁布0.9版，于1996年颁布了1.0版。在欧洲，英国、荷兰和法国带头，开始联合研制欧洲共同的安全评测标准，并于1991年颁布ITSEC(信息技术安全标准)。1993年，加拿大颁布CTCPEC(加拿大可信计算机产品评测标准)。1993年，美国国防部国防信息系统局又提出在C4I系统(Command，Control，Communication，Computer，and Intelligence System)上采用多级安全(MLS)技术与概念。在美国，信息和信息系统是由总统亲自领导的，投入力度相当可观。美国已经颁布了《计算机安全法》，日本也颁布了《反黑客法》。国际间的合作也已开始进行，2000年5月，在法国巴黎举行的《政府机构和私营部门关于网络空间安全和信任对话》会议，就是世界上首次以打击网络犯罪为主要内容的国际性会议。同时，一些大的跨国公司在信息和信息系统安全方面推出了新的技术和产品。例如：HP公司领导发布的X/Open Security Branding计划(1996年3月推出)，推出了ICF(国际密码架构)战略，联合其他合作伙伴共同占领广大的信息安全产品国际市场，并推出HPUXCMW B1级操作系统，通过TC－SE&ITSEC的评测。DEC公司推出安全级别为C2级的操作系统为Digital UNIX和Open VMS，推出的B1级/CMW级的操作系统是SEVMS和Digital MLS＋，通过了TCSEC和ITSEC的两个认证评测。还有网络监视器和防火墙产品，其中，Alta Vistaa Tunnel Personal Edition与Alta Vista Tunnel Workgroup Edition是两个著名产品。ORACLE公司的安全数据库是Trusted Oracle，是B2产品，在美国是用于军方的产品。还有B1级的ORACLE产品，通过了TCSEC和ITSEC的评测。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，中国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。从“七五”开始到“九五”期间，信息产业部15所太极计算机公司在网络安全方面进行了科研工作。在信息产业部15所在“九五”期间正在进行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网络接入交换设备、1000兆以太网络、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。北京信息工程学院、东大软件园区、中国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。

世界各国的信息安全技术水平可以划分为三类：一是信息化水平较高，信息安全保障水平相应较高的国家，如美国；二是信息化起步较晚，但已经达到一定程度的国家，其信息安全保障也相应具备了一定的基础，如中国；三是信息化刚刚起步，甚至没有起步，其信息安全保障几乎处于空白状态，如一些发展中国家。从总体上来说，即便是信息安全保障最发达的国家，也仍然没有具备完全解决信息安全问题的能力，像美国白宫和美国军队的网站就经常受到不明身份黑客的破译攻击而出现瘫痪、泄密等问题。在与信息安全破坏者的斗争中，目前全世界都处于被动的局面，这也决定了信息安全技术具有较大的发展空间。目前信息安全技术处于领先的国家主要是美国、法国、以色列、英国、丹麦、瑞士等，一方面这些国家在技术方面特别是在芯片技术上有着一定的历史沉积，另一方面这些国家信息安全技术的应用，例如电子政务、电子商务、企业信息化等起步较早，应用比较广泛。它们的领先优势主要集中在防火墙、入侵监测、漏洞扫描、防杀毒、身份认证等传统的安全产品上。而在注重防内兼顾防外的信息安全综合审计上，国内的意识理念早于国外，产品开发早于国外，目前在技术上有一定的领先优势。

就我国目前的情况而言，不论是政府部门还是科研机构都意识到信息安全事关国家安全，也给予了足够的重视，但是还存在以下几个方面的弱点：

1. 信息安全的观念有待加强

我国多数民众都存在着一种重视硬件忽视软件、重视软件开发忽视安全建设的错误倾向，导致在信息安全领域存在以下不足：

- ▶ 安全意识淡薄，管理措施不到位；
- ▶ 缺乏权威领导机构；
- ▶ 缺乏统一的、全局的安全规划；
- ▶ 缺乏有效的监管措施和手段；
- ▶ 缺乏专业的信息安全人才和专业队伍；
- ▶ 缺乏权威的安全评估机构和安全标准；
- ▶ 缺乏安全方面的立法，尚未把信息安全提高到法律的高度。

对信息安全这一涉及国家安全的战略性问题，我们不能“临渴掘井”，必须“未雨绸缪”，否则将可能给国家造成灾难性后果。

2. 客观上受制于技术水平

我国电子信息领域基础技术薄弱，制约了与信息安全相关产业的发展。我国尚没有充分掌握信息安全的核心技术，信息安全产品大多依赖进口。

3. 受政治等因素的影响，尤其应重视安全问题

美国是当今世界唯一的超级大国，在经济、技术、军事各方面具有压倒性优势。如果根据信息技术和信息经济的强弱对世界上的国家分类，那美国也是唯一的信息超级大国。美国为达到称霸世界目的，凭借信息技术优势，通过出口信息安全产品来达到控制、获取别国信息的目的。它起初限制 40 位密钥长度以上的密码产品出口，后来又同意具有密钥托管或密钥恢复功能的强密码产品出口，这些都是美国政府可以控制和解读的。此外，在

密码芯片和操作系统中可能隐藏着尚未为人们发现的、危险性更大的“后门”和“特洛伊木马”。一旦发生重大国际冲突，那些隐藏的“特洛伊木马”可能在某些秘密指令下激活起来，破坏、篡改或窃取信息系统中的重要信息。由于历史和意识形态方面的原因，中国和美国在许多方面存在很大的分歧，两国关系经常会出现不稳定的情况，美国对中国技术出口的限制尤其严厉。小布什政府上台后更是有把中国看成是战略对手的趋向。美国民间对中国存在偏见的也大有人在。比如微软公司的 Windows 操作系统在并不富裕的中国的售价是富裕的发达国家售价的一倍多，这是信息领域明目张胆的掠夺。在这样的国际背景下，我国信息安全的外部环境并不好，因此更应注重信息安全建设，以免在关键时刻受制于人！

4. 我国安全技术研究力量有限

我国国内信息安全研究力量分散，投入不足，现有研究仅能满足封堵已发现的安全漏洞，无法从根本上解决国家信息安全问题，更不要说形成反击能力。为此，应跟踪研究国际最新技术动态，努力吸取国外信息安全的先进技术和经验，不断创新，独立自主地发展我国的信息安全技术；加强对信息安全的支持力度，凝聚国内信息安全方面优秀人才，建设信息安全专业队伍；加强对信息安全体系、信息安全发展战略、安全核心技术、密码理论和应用技术、信息安全检测和监控技术以及病毒防治等研究，为我国的信息安全构筑起可靠屏障。

（二）信息安全技术发展趋势

在信息交换中，“安全”是相对的，而“不安全”是绝对的，随着社会的发展和技术的进步，信息安全标准不断提升，因此信息安全问题永远是一个全新的问题。“发展”和“变化”是信息安全的最主要特征，只有紧紧抓住这个特征才能正确地处理和对待信息安全问题，以新的防御技术来阻止新的攻击方法。信息安全技术的发展呈现如下趋势：

1. 信息安全越来越重要

信息安全系统的保障能力是 21 世纪综合国力、经济竞争实力和民族生存能力的重要组成部分。因此，必须努力构建一个建立在自主研究开发基础之上的技术先进、管理高效、安全可靠的国家信息安全体系，以有效地保障国家的安全、社会的稳定和经济的发展。信息安全是一个综合的系统工程，需要诸如密码学、传输协议、集成芯片技术、安全监控管理及检测攻击与评估等一切相关科技的最新成果的支持。

2. 信息安全标准在不断变化

应根据技术的发展和实际社会发展的需要不断更新信息安全标准，科学合理的安全标准是保障信息安全的第一步，需要无限追求如何在设计制作信息系统时就具备保护信息安全的体系结构，这是人们长期追求的目标。

3. 信息安全概念在不断扩展

安全手段需随时更新。人类对信息安全的追求过程是一个漫长的深化过程。信息安全的含义包括了信息的保密性、信息的完整性、信息的可用性、信息的可控性、信息行为的不可否认性。随着社会信息化步伐的加快，信息安全至少需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术的研究。