464

信息系统安全系列

信息系统安全

戴宗坤　罗万伯　等编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书从人、网络和运行环境结合的角度，将利用开放系统互连技术构成的信息系统的安全问题作为一个体系进行描述，突破了此前单纯从一个或几个方面阐述信息系统安全问题的传统思维模式。本书信息量极大，涉及信息系统及其与安全问题相关的多学科领域的基础知识和技术方法。本书内容主要包括信息安全机制、信息安全服务和信息安全管理在开放互连运行环境下如何构成信息系统安全体系的基本原理、方法和策略。

本书内容全面、文字流畅、表达准确，既可作为高等院校信息安全相关专业的本科生、研究生的教材或指定参考书，也可供从事信息系统及其与安全有关的教学人员、科研人员、工程技术人员以及信息技术管理人员参考。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目(CIP)数据

信息系统安全/戴宗坤等编著 .—北京：电子工业出版社，2002.11
(信息系统安全系列)
ISBN 7-5053-8089-3

Ⅰ.信… Ⅱ.戴… Ⅲ.信息系统—安全技术 Ⅳ.G202

中国版本图书馆 CIP 数据核字(2002)第 084428 号

责任编辑：刘宪兰　章海涛　　特约编辑：明足群
印　　刷：北京东光印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：31.5　字数：789.4 千字
版　　次：2002 年 11 月第 1 版　2002 年 11 月第 1 次印刷
印　　数：5 000 册　定价：39.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：(010)68279077

目　录

第1章 概 论

1946年，世界上第一台真正的电子计算机ENIAC在美国宾夕法尼亚州立大学诞生，信息技术的发展进入一个新阶段。自那以后，人类处于一个大变革的时代，作为社会发展三要素的物质、能源和信息的关系发生了深刻的变化。此前处于从属地位和起隐性作用的信息要素，终于在计算机技术和网络通信技术的推动下，迅速成为支配人类社会发展进程的决定性力量之一。人类开始从主要依赖物质和能源的社会步入物质、能源和信息资源三位一体的社会。在这种宏观背景下，首先是一些发达国家掀起了以发展信息科技、开发利用信息资源来促进社会、经济和文化进步的浪潮，从而启动了从工业化社会迈向信息化社会的进程。

纵观20世纪特别是后半叶的信息技术发展历史，从20世纪40年代以前的电话、电报、无线电广播和通信等，到电子管、晶体管、集成电路、激光、计算机、卫星通信、移动通信、局域网、广域网、因特网和虚拟现实技术等，差不多每十年就有与信息技术有关的、影响深远的重大创新和技术成就出现。近一二十年来，微电子技术和激光技术的发展，推动了大规模、超大规模集成电路和超大容量存储介质的发展和应用，信息处理设备呈现体积小型化、微型化和功能集成化、人性化的趋势；与此同时，通信技术和通信协议的发展推动了信息的高速传输和信息资源的广泛共享。信息技术的发展和应用加快了各种新技术、新知识、新文化的传播，深入到社会、政治、军事、经济、文化、医疗、社会保障、交通、通信、商务、生产、学习、交流和日常生活等各个领域和方面，深刻地影响着社会各阶层、各团体、每个人以及各个政体、国家自身内部以及相互之间关系的思维方式、行为方式和观念的变化。

以计算机及其外围设备为信息处理中心，以计算机网络作为信息传播平台，以有线和无线介质作为信息传输媒体的信息系统，正在进入人类社会的各个领域。现在，没有人怀疑计算机信息系统的应用价值和意义，因为人们正在自觉和不自觉地接受计算机信息系统“替我们干什么”和“要我们干什么”这一现实，并且根据自己对信息技术的理解“体会到”和“感知到”计算机信息系统在“迫使”人们改变传统的思维模式和行为方式。也许，不是所有的人能说清楚“功能如此强大的计算机信息（系统）技术一定于我有益”，但是几乎所有人都会感受到一种无形的巨大推力，让你去认识它、理解它，即使不情愿，将来也得“顺从它”。这就是潮流。

那么，信息、信息技术和信息系统到底是什么呢？如何最大限度地利用信息系统为我们“创造价值”，为我们服务而不招致损失或使损失最小呢？本章力图为其给出比较系统的基础性概念和理论知识。

1.1 信息的概念及其他

“信息”一词古已有之。在人类社会早期的日常生活中，人们对信息的认识比较广义而模糊，对信息和消息的含义没有明确界定。到了20世纪尤其是中期以后，现代信息技术的

试读结束：需要全本请在线购买： www.ertongbook.com

飞速发展及其对人类社会的深刻影响，迫使人们开始探讨信息的准确含义。

一般意义上的信息定义认为，信息是事物运动的状态与方式。如果引入必要的约束条件，则可形成信息的概念体系。信息有许多独特的性质与功能，也可以进行测度。正因为如此，才导致信息科学的出现。

1.1.1 信息的经典定义

1928 年，哈特雷（L.V.R.Hartley）在《贝尔系统电话杂志》上发表了题为《信息传输》的论文。他在文中将信息理解为选择通信符号的方式，且用“选择的自由度”来计量这种信息的大小。他注意到，任何通信系统的发信端总有一个字母表（或符号表），发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符号序列的过程。假定这个符号表一共有 S 个不同的符号，发送信息选定的符号序列一共包含 N 个符号，那么，这个符号表中无疑有 S^N 种不同符号的选择方式，也可以形成 S^N 个长度为 N 的不同序列。这样，就可以把发信者产生信息的过程看做从 S^N 个不同的序列中选定一个特定序列的过程，或者说是排除其他序列的过程。

然而，用“选择的自由度”来定义信息存在着局限性，主要表现在：一方面，这样定义的信息没有涉及信息的内容和价值，也未考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主体作为限制条件。因此，这样的信息只是一种认识论意义上的信息。

1948 年，香农（C.E.Shannon）在《通信的数学理论》一文中，在信息的认识方面取得重大突破，堪称信息论的创始人。香农的贡献主要表现在推导信息测度的数学公式上，发明了编码的三大定理，为现代通信技术的发展奠定了理论基础。

香农发现，通信系统所处理的信息在本质上都是随机的，可以运用统计方法进行处理。他指出，“一个实际的消息是从可能的消息集合中选择出来的，而选择消息的发信者又是任意的，因此，这种选择就具有随机性”。这是一种大量重复发生的统计现象。

香农对信息的定义同样具有局限性，主要表现在：这一概念同样未能包含信息的内容与价值，只考虑了随机型的不定性，未能从根本上回答信息是什么的问题。

1948 年，就在香农创建信息论的同时，维纳（N.Wiener）出版了专著《控制论——动物和机器中的通信与控制问题》，并且创立了控制论。后来，人们常常将信息论、控制论以及系统论合称为“三论”，或统称为“系统科学”或“信息科学”。

维纳从控制论的角度认为，“信息是人们在适应外部世界，并且使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称”。他还认为，“接收信息和使用信息的过程，就是适应外部世界环境的偶然性变化的过程，也是我们在这个环境中有效地生活的过程”。维纳的信息定义包含了信息的内容与价值，从动态的角度揭示了信息的功能与范围。但是，人们在与外部世界的相互作用过程中，同时也存在着物质与能量的交换，不加区别地将信息与物质、能量混同起来是不确切的，因而也有局限性。

1975 年，意大利学者朗高（G.Longo）在《信息论：新的趋势与未决问题》一书的序中指出，信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身。无疑，“有差异就是信息”的观点是正确的，但“没有差异就没有信息”的说法却不够确切。譬如，我们碰到两个长得一模一样的人，他（她）们之间没有什么差异，但会马上

联想到“双胞胎”这样的信息。可见，“信息就是差异”也有其局限性。

据不完全统计，信息的定义有 100 多种，它们都从不同侧面、不同层次揭示了信息的特征与性质，但也都有这样或那样的局限性。信息作为物质世界的三大组成要素之一，其定义的适用范围是非常宽的。上述几种经典定义也只适合特定范围或层次，是人们在探索信息的过程中所形成的几种含金量高的认识积淀。

1.1.2 与现代通信有关的信息定义

通信领域对信息的研究有着悠久的历史，信息科学的出现正是通信理论研究的最重要的成果之一。1988 年，中国学者钟义信在《信息科学原理》一书中，认为信息是事物运动的状态与方式，是事物的一种属性。信息不同于消息，消息只是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息；可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是序化的信息，并非所有的信息都是知识。他还通过引入约束条件推导了信息的概念体系，对信息进行了完整而准确的论述。

通过比较，中国科学院文献情报中心孟广均研究员等在《信息资源管理导论》一书中认为，“作为与物质、能量同一层次的信息的定义，信息就是事物运动的状态与方式”。因为这个定义具有最大的普遍性，不仅涵盖所有其他的信息定义，而且通过引入约束条件还能转换为所有其他的信息定义。

1.1.3 信息的性质

信息来源于物质，不是物质本身；信息也来源于精神世界，又不限于精神的领域。信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，它们主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性等。

信息系统安全将处理与信息依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性有关的问题。

1.1.4 信息的功能

信息的功能是信息属性的体现。相对于信息的本质属性和一般属性，信息的功能也可分为两个层次：信息的基本功能在于维持和强化世界的有序性；信息的社会功能则表现为维系社会的生存，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在下述 5 个方面。

① 信息是宇宙万物有序运行的内在依据。信息源于物质的运动，早在生命现象出现之前，自然界中无机物之间、无机物及其周围环境之间就存在着相互作用，存在着运动、变化的过程，因而也存在着信息的运动过程。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，缺少信息的世界则是混乱的世界。

② 信息是人类认识世界和改造世界的中介，在于实现人类与自然界的沟通。人类通过

自己的感觉器官，从物质世界中感知和提取信息；通过大脑的加工，以信息输出的形式作用于物质世界，达到改造的目的。信息始终是这个过程的中介和替代物。

③ 信息是社会生存与发展的动因。信息交流是人类社会活动赖以形成、维系和发展的根本保证。由于社会内部的信息交流，使后人可以在前人的肩膀上起步。因此，信息本身也是社会前进与发展的基石，是人类进化的动力。

④ 信息是智慧之源，是人类的精神食粮。人的思维和智慧是信息过程的产物，不能想像没有信息的生活。

⑤ 信息是管理的灵魂。管理一直是人类的一项经常性的社会活动，是一个有序化的过程。管理主体向管理客体传递信息、监督客体的运行状态，收集反馈信息，不断地做出调整，以保证目标的实现。管理最重要的职能之一是决策。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、全面且及时的信息。

信息还是一种重要的社会资源。现代社会将信息、材料和能源看做支持社会发展的三大支柱，这说明了信息在现代社会中的重要性。

信息系统安全的任务是确保信息功能的正确实现。

1.2　信息技术

1.2.1　信息技术的产生和发展

任何技术都产生于人类社会实践活动的实际需要。按照辩证唯物主义观点，人类的一切活动都可以归结为认识世界和改造世界。人类认识世界和改造世界的过程，从信息的观点来分析，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。

“科学”是扩展人类各种器官功能的原理和规律，而“技术”则是扩展人类各种器官功能的具体方法和手段。从历史上看，人类在很长一段时间里，为了维持生存而一直采用优先发展自身体力功能的战略，因此材料科学与技术和能源科学与技术也相继发展起来。与此同时，人类的体力功能也日益加强。信息虽然重要，但在生产力和生产社会化程度不高的时候，人们仅凭自身的信息器官的能力，就足以满足当时认识世界和改造世界的需要了。随着生产斗争和科学实践活动的深度和广度的不断发展，人类的信息器官功能已明显滞后于行为器官的功能了。例如人类要“上天”、“入地”、“下海”、“探微”，但其视力、听力、大脑存储信息的容量、处理信息的速度和精度，越来越不能满足同自然作斗争的实际需要了。到了这个时候，人类才把关注的焦点转移到扩展和延长自己信息器官的功能方面。

从 20 世纪 40 年代起，人类在信息的获取、传输、存储、处理和检索等方面的技术与手段，以及利用信息进行决策、控制、指挥、组织和协调等方面的原理与方法，都取得了突破性的进展，且是综合性的。这些事实从侧面说明了当代技术发展的主流已经转向信息科学技术。

1.2.2 信息技术的内涵

对于信息技术，目前还没有一个准确而又通用的定义。为了研究和使用的方便，学术界、管理部门和产业界等都根据各自的需要与理解给出了自己的定义，估计有数十种之多。信息技术定义的多样化，不仅反映在语言、文字和表述方法的差异上，而且也有对信息技术本质属性理解方面的差异。

目前，比较有代表性的信息技术定义主要有以下6种：

① 信息技术是基于电子学的计算机技术和通信技术的结合而形成的对声音、图像、文字、数字和各种传感信号的信息进行获取、加工处理、存储、传播和使用的能动技术。

② 信息技术是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频以及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。

③ 信息技术是人类在生产斗争和科学实验中，认识自然和改造自然的过程中所积累起来的获取信息、传递信息、存储信息、处理信息以及使信息标准化的经验、知识、技能，以及体现这些经验、知识、技能的劳动资料有目的的结合过程。

④ 信息技术是在信息加工和处理过程中使用的科学、技术与工艺原理和管理技巧及其应用，以及与此相关的社会、经济与文化问题。

⑤ 信息技术是管理、开发和利用信息资源的有关方法、手段与操作程序的总称。

⑥ 信息技术是能够延长或扩展人的信息能力的手段和方法。

上述定义都试图从功能方面揭示信息技术的本质。从语法角度来看，“信息技术”作为专门术语，其概念的本质是“技术”而非“信息”。结合本书论述的对象和范围，我们将信息技术的内涵限定在上述第②种定义以内，即强调信息技术是获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频和语音信息，以及提供完成这些活动的信息设备和提供信息服务两大方面的方法与设备的总称。

1.3 信息系统

1.3.1 信息系统的基本内涵

与“信息”、“系统”的定义具有多样性一样，信息系统这种与“信息”有关的“系统”，其定义也远未达成共识。比较流行的看法有以下4种。

《大英百科全书》把“信息系统”解释为“有目的、和谐地处理信息的主要工具是信息系统，它对所有形态（原始数据、已分析的数据、知识和专家经验）和所有形式（文字、视频和声音）的信息进行收集、组织、存储、处理和显示”。

巴克兰德（M.Buckland）认为，信息系统是“提供信息服务，使人们获取信息的系统，如管理信息服务、联机数据库、记录管理、档案馆、图书馆、博物馆等”。

达菲（N.M.Dafe）等认为，信息系统大体上是“人员、过程、数据的集合，有时候也包括硬件和软件。它收集、处理、存储和传递在业务层次上的事务处理数据和支持管理决策的信息”。

中国学者吴民伟认为，信息系统是“一个能为其所在组织提供信息，以支持该组织经营、管理、制定决策的集成的人—机系统。信息系统利用计算机硬件、软件、人工处理、分析、计划、控制和决策模型，以及数据库和通信技术”。

可见，对信息系统的定义仍是同中有异，异中有同。不过，若将信息系统涉及的功能与范围加以适当界定，仍可大体统一在两种认识上。广义理解的信息系统包括的范围很广，各种处理信息的系统都可算作信息系统，包括人体本身和各种人造系统。狭义理解的信息系统仅指基于计算机的系统，是人、规程、数据库、硬件和软件等各种设施、工具和运行环境的有机集合，它突出的是计算机和网络通信等技术的应用。就本书研究的内容而言，我们将信息系统限于后一种定义的范畴。

1.3.2 信息系统的发展

信息系统从概念上讲，在计算机问世之前业已存在，但它的加速发展和日益为人瞩目却是在计算机和网络广泛应用之后。自 20 世纪初泰罗创立科学管理理论以来，管理科学与方法技术得到迅速发展。在与统计理论和方法、计算机技术、通信技术等相互渗透、相互促进的发展过程中，信息系统作为一个专门领域迅速形成。

作为用计算机处理信息的人—机系统的信息系统，它在近半个世纪中得到迅猛发展。

电子数据处理系统（EDPS，Electronic Data Processing Systems）：电子数据处理系统是用计算机代替以往人工进行事务性数据处理的系统，所以也有人称其为事务处理系统（TPS，Transaction Processing Systems）。这一阶段从 20 世纪 50 年代初，商界第一次用计算机处理工资单、财务报表和账单等开始。电子数据处理系统有一些缺陷，如受限于当时计算机的能力和人们对计算机的认知，完全模拟人工系统，数据收集因为速度慢且容易出错，成为该系统最薄弱的环节。

管理信息系统（MIS，Management Information Systems）：管理信息系统是在事务处理系统基础上发展起来的第二代信息系统，但两者有显著的区别：事务处理系统是处理和获取数据，仅涉及一个部门内的操作性活动；管理信息系统则为管理提供信息，是一个部门的管理工具，它强调管理方法和技术的应用，强调把信息处理的速度和质量扩大到组织机构的所有部门，从而增强组织机构中各职能部门的管理效率和能力。

决策支持系统（DSS，Decision Support Systems）：决策支持系统的概念是美国学者莫顿（S.Morton）于 20 世纪 70 年代初首次明确提出的。它是辅助决策工作的一种信息系统，其重点在“支持”而非决策工作的自动化。

办公自动化系统（OAS，Office Automation Systems）和多媒体信息系统（MMIS，Multimedia Information Systems）：严格来说，办公自动化系统和多媒体信息系统只是前文所述的电子数据处理系统（或事务处理系统）、管理信息系统和决策支持系统等几类信息系统的一种综合应用，不可简单地把这两者称为新型的信息系统。但是，正是办公自动化系统在 20 世纪 80 年代的广泛应用以及多媒体信息系统在 20 世纪 90 年代的蓬勃发展，才使信息系统这一领域更加引人注意，而多媒体信息系统自身也成为各类信息系统应用的方向。

1.4 信息系统安全

1.4.1 信息安全与信息系统安全

信息安全是一个更为广泛和抽象的概念。长期以来，当人们谈及与计算机网络（或因特网）有关的信息系统的安全时，往往笼统地称为信息安全。仔细琢磨起来，信息安全与信息系统安全是有概念上的区别的。一般来说，当人们谈及与信息内容安全、计算机通信安全、计算机网络安全和因特网接入安全等问题时，都会用信息安全来说明其中的部分问题。但信息安全并不代表、也不说明任何具体的个体或系统与安全有关的问题。因此，信息安全更多的是一种概念性的东西。

信息系统安全则是确保信息系统结构安全，与信息系统相关的元素安全，以及与此相关的各种安全技术、安全服务和安全管理的总和。因此，信息系统安全更具有体系性、可设计性、可实现性和可操作性。本书将信息系统的概念限制于基于开放系统互连和计算机网络的复杂巨系统，以此为基础开展信息系统安全的研究。

1.4.2 信息系统安全的内涵

本书中将信息系统安全的内涵定义为：确保以电磁信号为主要形式的，在计算机网络化系统中进行获取、处理、存储、传输和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性的，与人、网络、环境有关的技术和管理规程的有机集合。这里的人指信息系统的主体，包括各类用户、支持人员以及技术管理和行政管理人员；网络则指以计算机、网络互联设备、传输介质及其操作系统、通信协议和应用程序所构成的物理的和逻辑的完整体系；环境则指系统稳定和可靠运行所需要的保障系统，包括建筑物、机房、动力保障与备份以及应急与恢复系统。

从系统过程与控制角度看，信息系统安全就是信息在存取、处理、集散和传输中保持其机密性、完整性、可用性、可审计性和抗抵赖性的系统辨识、控制、策略和过程。

系统辨识是近代控制理论的一个方面，它研究如何建立系统的数学模型，内容包括模型类型的确定、参数估计方法和达到高精度估计的实验设计方法。

控制是指信息系统根据变化进行调整，使信息系统保持特定的状态，即便信息系统处于动态平衡的状态。因此，调整的方向和目标是使信息系统始终处于风险可接受的范围内，并且逐步收敛至风险趋于最小。

策略就是针对信息系统安全面临的系统脆弱性和各种威胁，进行安全风险分析，制定安全目标，建立安全模型和安全等级，提出控制对策，并且对信息系统安全进行评估、制定安全保障和安全仲裁等对策。

过程是指信息系统状态的变化在时间上的持续和在空间上的延伸，过程和状态不可分割，两者相互依存、相互作用和相互制约。信息系统的状态决定和影响着过程，而过程又决定和影响着新的状态（或过程）。

试读结束：需要全本请在线购买： www.ertongbook.com

上述研究方法有两个基本要素：一是将信息系统的安全作为状态来研究，二是将信息系统安全作为对状态的控制调节来研究。控制调节的目的就是使系统稳定在某一特定状态内。

1.4.3 信息系统安全的方法论

信息系统安全是一个多维、多层次、多因素、多目标的体系。虽然信息系统安全的惟一和最终的目标，是为了保障信息内容在系统内的任何地方、任何时候和任何状态下的机密性、完整性和可用性，但是离开信息系统安全的体系，孤立和单纯地去寻求直接保护信息内容的方式，显然是舍本求末。另一方面，信息系统是依附于国家、组织机构和个人的，它是国家、组织机构和个人应用业务和管理体系的网络化映射，以及集体智慧、个人思维和行为能力的延伸。因此，需要将信息系统安全的完整内涵与信息安全方法论匹配起来，有必要从系统工程的角度去理解和构造信息系统安全体系或模式。

信息系统安全工程方法的要点是：首先，信息系统是一项系统工程。这项系统工程由信息系统功能性工程和确保信息系统按照管理者意志可靠、稳定、有序地实现其功能的安全性工程，有机地组合起来。第二，信息系统功能性工程的各组件要素应具备支持功能和履行功能的能力。第三，对信息系统功能性工程各组件要素，在实现系统功能过程中确保信息内容机密性、完整性和可用性可能存在的自身固有的脆弱性、缺陷和漏洞，以及可能遭遇的来自系统内部和外部的对系统的骚扰、入侵，或者对信息的窃听、截获、注入和修改等威胁和攻击进行分类、分等级排列和分析。第四，针对前述问题，信息系统安全性工程从物理安全、环境安全、操作系统安全、通信安全、传输安全、应用安全以及用户安全等方面形成安全服务体系框架，恰当地采用各种安全技术配置在相应的信息系统功能性工程各组件要素上，直接或间接提供必要的安全服务以保证功能性组件要素正常、稳定和可靠地履行其功能。显然，信息系统安全性工程是一个嵌入到功能性工程中的集中管理分布式控制体系，它是功能性工程的保障体系。这里有两个问题需要特别强调：一是系统工程（含安全性工程）内各组件要素可以是物化的设施和实体，也可以是虚化的设施和实体；二是各组件要素所提供的安全服务的强度级别应高于或等于信息系统总的安全强度级别。

1.4.4 信息系统安全与保密

就信息安全和信息系统安全的内涵而言，保证信息（内容）的保密性是系统安全的基本和首要目标之一。从信息保密性角度来看，信息（系统）安全涵盖信息保密的内容。但是在国家管理中，保密作为一个特殊、独立的概念，在各个国家的各个历史进程中，作为涉及国家安全、社会稳定的信息和控制函数，具有对时间、空间的强制性和时效性特点。因此，与一般意义的信息安全中的机密性比较，虽然都是针对未授权者而言的，但保密却具有与一般意义上的信息保密性不同的其他特殊含义。同时，保密技术还具有自己相对独立、更为广泛和完整的体系以及国家对抗性特点，由此决定了保密技术和保密管理体系本身具有国家机密性特点。

在强调信息系统安全和保密时，是将保密作为管理策略和安全策略的一部分而不仅是信息保密（机密）性指标来定义的。作为管理策略和安全策略，保密涉及对信息系统的信息密级进行划分和管理，对涉密网络和非涉密网络进行界定和管理，对保密技术和产品进行保

密管理，对具有对抗性和敏感性的保密技术主体和客体实施检查、监督和控制等。显然，作为管理策略和安全策略，保密是信息系统安全的功能性和管理性保障。国家对保密工作历来十分重视，从技术到管理形成了一个完整的体系。保密在信息系统安全中的作用和地位是不可取代的。

1.5 信息系统风险和安全需求

安全风险是信息系统各组成要件在履行其应用功能过程中，在机密性、完整性和可用性等方面存在的脆弱性（点），以及信息系统内部或外部的人们利用这些脆弱性（点）可能产生的违背信息系统所属组织安全意志的后果。安全需求则是对抗和消除安全风险的必要方法和措施。安全需求是制定和实施安全策略的依据。

就信息系统安全体系而言，由于安全风险和安全策略是矛盾的双方，因此安全风险和安全策略是对立统一的。安全风险是安全需求的催生剂，安全策略是安全风险的制约者或终结者。由于安全风险具有时间动态性和空间分布性，因此安全需求也必须是时间动态和空间分布的。一般来说，由于人们对安全风险有一个认识过程，因而安全需求总是滞后于安全风险的发生和发展。信息系统安全体系的研究者和设计者的最高目标，则是从研究信息系统风险的一般规律入手，认识和掌握信息系统风险状态和分布情况的变化规律，提出安全需求，建立具有自适应能力的信息系统安全模型，从而驾驭安全风险，使信息系统风险控制在可接受的最小限度内，并渐近于零风险。实际上，零风险永远是人类追求的极限目标，因此信息系统安全体系的成功标志是风险的最小化、收敛性和可控性，而不是零风险。

信息系统及其组件的脆弱性（点）是安全风险产生的内因，威胁和攻击则是安全风险的外因。从另一个角度看，安全风险的客体是系统及其组件的脆弱性（点），安全风险的主体是针对客体所进行的威胁和攻击。可见，当安全风险的因果或主客体在时空上一致时，风险就危及或破坏了系统安全，或者说信息系统处于不稳定、不安全状态中。这种情况正是信息系统安全必须规避的。

1.5.1 信息系统风险概览

1. 信息系统组件固有的脆弱性和缺陷

信息系统多组件在设计、制造和组装中，由于人为和自然的原因，可能留下各种隐患。

（1）硬件组件

信息系统硬件组件的安全隐患多数来源于设计，主要表现为物理安全方面（如物理可存取和电磁兼容方面等）的问题。由于这种问题是设计时所遗留的固有问题，一般除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此，在自制硬件和选购硬件时应尽可能减少或消除这类安全隐患。

（2）软件组件

软件组件的安全隐患来源于设计和软件工程实施中的遗留问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余以及软件过长过大，不可避免地存在安全脆

弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中的软件系统内部逻辑混乱，导致垃圾软件，这种软件从安全角度看是绝对不可用的。

软件组件可分为操作平台软件、应用平台软件和应用业务软件三类，以层次结构构成软件组件体系。操作平台软件处于基础层，它维系着系统硬件组件协调运行的平台，因此平台软件的任何风险都可能直接危及或被转移或延伸到应用平台软件。对信息系统安全所需的操作平台软件的安全等级要求，不得低于系统安全等级要求；特别是信息系统的安全服务组件的操作系统安全等级，必须至少高于系统安全一个等级。因此，强烈建议安全服务组件的操作系统不得直接采用商业级和/或普遍实用的操作系统。

应用平台软件处于中间层次，它是在操作平台支撑下运行的支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可以直接危及或传递给应用业务软件。因此，应用平台软件的安全特性至关重要，在提供自身安全保护的同时，应用平台软件还必须为应用业务软件提供必要的安全服务功能。

应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险，都直接表现为信息系统的风险。因此，其安全功能的完整性以及自身的安全等级，必须大于系统安全的最小需求。一般来说，外购经过资质认证的商业化应用业务软件比自制应用业务软件更安全些。

（3）网络和通信协议

在当今的网络通信协议中，局域网和专用网络的通信协议具有相对封闭性，因为它们不能直接与异构网络连接和通信。这样的“封闭”网络本身基于两个原因，比开放式的因特网的安全特性好：一是网络体系的相对封闭性降低了从外部网络或站点直接攻入系统的可能性（但信息的电磁泄露性和基于协议分析的搭线截获等问题仍然严重存在）；二是专用网络自身具有较为完善、成熟的身份鉴别，访问控制和权限分割等安全机制。

安全问题最多的，还是基于 TCP/IP 协议栈的因特网及其通信协议。因为因特网本身是一个没有明确物理界限的网际，其中的国与国之间、组织与组织之间、个人与个人之间的网络界限是依靠协议、约定和管理关系进行逻辑划分的，因而是一种虚拟的网络现实；而且支持因特网运行的 TCP/IP 协议栈在设计的当初原本只考虑了互联互通和资源共享的问题，并未考虑也无法兼容解决来自网际的大量安全问题。

因特网何以存在如此多的安全隐患，TCP/IP 协议栈到底有哪些脆弱性和漏洞？要理解与因特网有关的安全脆弱性和漏洞存在的原因和分布情况，得从网络技术发展历史和 TCP/IP 协议栈的研究初衷、应用背景以及发展驱动力等方面谈起。

最初的计算机网络建设，遵循的思路是“局域网（LAN）—城域网（MAN）—广域网（WAN）”扩张模式。网络的体系结构及其通信协议、网络操作系统也因开发商不同而不同，且以少数垄断企业的网络及其通信协议标准为事实上的工业标准，比较典型的网络体系有 IBM/SNA，Novell/NetWare，DECnet 等。作为公共数据基础通信设备的网络则使用 X.25，FR，ISDN，DDN，PSTN 等交换技术，信息访问的方式主要有主机方式和客户/服务器（C/S）方式等。虽然 ISO 早在 1978 年就制定了 OSI 七层网络通信标准，随后陆续推出相应的安全体系结构及其安全服务和安全机制标准，但由于这些标准过于复杂和完整，加上网络技术发

展太快以及商业利益的驱动，迄今为止实际上没有真正的产品完全遵从这些标准，世界上的大多数网络仍使用的是几家网络公司事实上的“工业标准”。即使在广域网和城域网中，也基本上使用的是各种自成体系的专用网络及其通信技术。在这种网络环境下的内部通信和信息共享可以遵从各自体系的同一标准，当要在两种异构网络之间进行通信时，则困难很大，主要问题在于通信协议和数据交换格式不同。这一问题成了异构网络和异型计算机之间通信与信息共享的技术屏障。这一现象在20世纪70年代至80年代初期被研究人员称为“信息孤岛”。

消除解决信息孤岛之间互联互通技术屏障的努力一直在进行。获得成功的是美国国防高级研究计划署（DARPA）于1973年启动的因特网计划。该计划原本用于解决军事部门内部各种计算机网络的互联问题，其互联的网络称为Internet DARPA。为此，组织了美国大学、研究机构、商业公司以及欧洲一些研究机构参加的研究活动，开发用于因特网的TCP/IP协议集。这个计划中第一个可运行的系统在1977年进行了演示，它包括ARPAnet、一个分组无线网、一个分组卫星网和Xerox公司研究中心的一个以太网等四个部分。其中ARPAnet运行得非常成功，于是DARPA不再将其作为实验网络，于1983年1月将其移交当时的国防通信局（DCA）进行控制和管理。在此基础上，组建了ARPA Internet，DCA要求所有互联的网络都使用TCP/IP协议栈。与此同时，DCA将ARPAnet一分为二，一个继续用于研究目的，仍叫ARPAnet，另一个用于军事目的，叫MILnet。这两个网络就是早期因特网的两个跨地区主干网络。此后，美国一些政府部门的网络，如ESnet，NSFnet和NASnet等纷纷接入ARPAnet。由于NSFnet运行非常成功，逐渐取代了ARPAnet而成为因特网的主干网，后来一段时间甚至成了因特网的代名词。美国国家科学基金会（NSF）在1990年制定的AUP（可接受的使用策略），促进了因特网商业连接服务机构的出现，逐步将原来只允许用于教育和科研的TCP/IP技术，扩大到用于世界许多地方的连接服务。此后，一些大的网络公司认识到因特网的巨大商业价值，推动了美国政府建立国家信息基础设施（NII），即所谓信息高速公路的建设。

基于TCP/IP协议簇的因特网技术的发展极为成功，其主要原因是它使用了统一和有效的用于网络互联的网络通信协议集TCP/IP，且被开发成为适用于各种软件平台，从而打破了异型计算机之间、异构网络之间互联互通的技术屏障；利用TCP/IP技术开发的形形色色的服务软件，使得通信和信息共享极为方便，吸引了横向、纵向各个层次的团体、个人用户；因特网的网络结构采用主干地区、园区的分层网络互联结构，其用户覆盖面极大，具有网络用户扩展的物理空间。以上三方面的积极因素推动了高速、宽带基础网络通信设备的建设，因特网技术市场和信息供求市场的规模效益又刺激了基于因特网技术的信息产业及用户市场像滚雪球一样扩张。

人们在享受因特网技术给全球信息共享带来的方便性和灵活性的同时必须认识到，因特网及其通信协议栈在开放网络环境下，其安全隐患也是全面而系统的。

总之，基于TCP/IP的因特网是在可信任网络环境中开发出来的成果，体现在TCP/IP协议上的总体构想和设计本身，基本未考虑安全问题。当我们在一个无网络边界的、互不信任的网络环境中认定安全脆弱性或安全漏洞的问题时，这在可信任的环境中并不是问题。TCP/IP协议最初设计的应用环境是美国国防系统的内部网络，这一网络环境是互相信任的。当其推广到全社会的应用环境之后，信任问题就发生了。因此，因特网充满安全隐患就不难

理解了。概括起来，因特网网络体系存在着如下 3 种致命的安全隐患。

1）缺乏对用户身份的鉴别

TCP/IP 协议的机制性安全隐患之一是缺乏对通信双方真实身份的鉴别机制。由于 TCP/IP 协议使用 IP 地址作为网络节点的惟一标识，而 IP 地址的使用和管理又存在很多问题，因而导致下列两种主要安全隐患。

① IP 地址是由 InterNIC 分发的，其数据包的源地址很容易被发现，且 IP 地址隐含所使用的子网掩码，攻击者据此可以画出目标网络的轮廓。因此，使用标准 IP 地址的网络拓扑对因特网来说是暴露的。

② IP 地址很容易被伪造和被更改，且 TCP/IP 协议没有对 IP 包中源地址真实性的鉴别机制和保密机制。因此，因特网上任一主机都可产生一个带有任意源 IP 地址的 IP 包，从而假冒另一个主机进行地址欺骗。

2）缺乏对路由协议的鉴别认证

TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，因此对路由信息缺乏鉴别与保护。可以通过因特网对路由信息修改网络传输路径，误导网络分组传输。

3）TCP/UDP 的缺陷

TCP/IP 协议规定 TCP/UDP 是基于 IP 协议上的传输协议。TCP 分段和 UDP 数据包是封装在 IP 包中在网上传输的，除可能面临 IP 层所遇到的安全威胁外，还存在 TCP/UDP 实现中的以下 3 种安全隐患。

① 建立一个完整的 TCP 连接，需要经历“三次握手”过程。在客户/服务器模式的“三次握手”过程中，假如客户的 IP 地址是假的，是不可达的。那么，TCP 不能完成该连接所需的“三次握手”，使 TCP 连接处于“半开”状态。攻击者利用这一弱点可以实施如 TCP SYN Flooding 攻击的“拒绝服务”攻击。

② TCP 提供可靠连接是通过初始序列号和鉴别机制来实现的。一个合法的 TCP 连接都有一个客户/服务器双方共享的惟一序列号作为标识和鉴别。初始序列号一般由随机数发生器产生，问题出在很多操作系统（如 UNIX）在实现 TCP 连接初始序列号的方法中，所产生的序列号并不是真正随机的，而是一个具有一定规律、可猜测或计算的数字。对攻击者来说，猜出了初始序列号并且掌握目标 IP 地址之后，就可以对目标实施 IP Spoofing 攻击，而 IP Spoofing 攻击很难检测，因此此类攻击危害极大。

③ 由于 UDP 是一个无连接控制协议，极易受 IP 源路由和拒绝服务型攻击。

在 TCP/IP 协议层结构中，应用层位于最顶部，因此下层的安全缺陷必然导致应用层的安全出现漏洞甚至崩溃；各种应用层服务协议（如 Finger，FTP，Telnet，E-mail，DNS，SNMP 等）本身也存在许多安全隐患，这些隐患涉及鉴别、访问控制、完整性和机密性等多个方面，极易引起针对基于 TCP/IP 应用服务协议和程序方面安全缺陷的攻击并且获得成功。

2. 威胁和攻击

（1）威胁与攻击分类

1）威胁

对数据通信系统的威胁包括：对通信或网络资源的破坏，对信息的滥用、讹用或篡改，对信息或网络资源的窃取和删除，信息被泄露；服务中断和被禁止等。

可将威胁分为偶发性与故意性两类，也可以用主动或被动方式对威胁进行分类。

① 偶发性威胁。偶发性威胁是指那些不带预谋企图的威胁。偶发性威胁的实例包括系统故障、操作失误和软件出错。

② 故意性威胁。故意性威胁的范围，可从使用易行的监视工具进行随意的检测，到使用特别的系统知识进行精心策划的攻击。一种故意的威胁如果实现，就可认为是一种“攻击”。

③ 被动性威胁。被动威胁是指这样一些威胁：它的实现不会导致对系统中所含信息或信息系统资源的任何修改，而且系统的操作与状态也不受改变。使用消极的搭线窃听办法以观察在通信线路上传送的信息就是被动威胁的一种实现。

④ 主动性威胁。对系统的主动威胁涉及对系统中所含信息或信息系统资源的篡改，或对系统的状态或操作的改变。一个非授权的用户不怀好意地改动路由选择表，就是主动威胁的一个例子。

2）几种特定类型的攻击

下面简要列举在数据处理与数据通信环境中特别关心的几种攻击。在下列各条中，出现“授权”与“非授权”两个术语。授权意指“授予权力”。这个定义包含两层意思：这里的权力是指进行某种活动的权力（如访问数据），这样的权力被授予某个实体、代理人或进程。于是，授权行为就是履行被授予权力（未被撤销）的那些活动。

① 冒充。冒充就是一个实体假装成另一个不同的实体。冒充常与某些别的主动攻击形式一起使用，特别是消息的重放与篡改。例如，鉴别序列被截获，且在一个有效的鉴别序列发生之后被重放。具有很少特权的实体，为了得到额外的特权可能使用冒充，装扮成具有这些额外特权的实体。

② 重放。当一个消息或部分消息，为了产生非授权的使用效果而被重复时便出现重放。例如，一个含有鉴别信息的有效消息可能为另一个实体所重放，目的是使它通过鉴别取得合法性（把它当做其他合法实体）。

③ 篡改。当传送的数据内容被改变而未发觉，并且导致一种非授权后果时便出现消息篡改。例如，消息“允许甲读机密文卷‘账目’”被篡改为“允许乙读机密文卷‘账目’”。

④ 服务拒绝。当一个实体不能执行它的正当功能，或它的动作妨碍别的实体执行它们的正当功能的时候，便发生服务拒绝。这种攻击可能是一般性的，如一个实体抑制所有的消息；也可能是有具体目标的，例如一个实体抑制所有流向某一特定目的端的消息（如安全审计服务信息）。这种攻击可以是对通信业务流的抑制，如本例中所述，或产生额外的通信业务流；也可能制造出试图破坏网络操作的消息，特别是网络具有中继实体，这些中继实体根据从别的中继实体那里接收到的状态报告，做出路由选择的决定。

⑤ 内部攻击。当系统的合法用户以非故意或非授权方式进行动作时，便出现内部攻击。多数已知的计算机犯罪都和使系统安全遭受损害的内部攻击有密切的关系。防止内部攻击的保护方法包括：对工作人员进行仔细审查并进行安全意识教育和安全操作训练；仔细检查硬件、软件、安全策略和系统配置，以便在一定程度上保证它们运行的正确性（称为可信功能度）；审计跟踪以提高检测这种攻击的可能性并高速安全策略。

⑥ 外部攻击。外部攻击可以使用的方法包括：搭线（主动的与被动的）；截获辐射；冒充系统的授权用户，或者冒充系统的组成部分；为鉴别或访问控制机制设置旁路等。

试读结束：需要全本请在线购买： www.ertongbook.com