普通高等教育“十一五”国家级规划教材

高等学校信息安全系列教材

信息系统安全理论与技术(第2版)

方勇 主编

刘嘉勇 周安民 欧晓聪 胡勇 吴少华 编著

高等教育出版社
Higher Education Press

普通高等教育“十一五”国家级规划教材
高等学校信息安全系列教材

信息系统安全理论与技术

（第2版）

方勇　主编

刘嘉勇　周安民　欧晓聪　胡勇　吴少华　编著

高等教育出版社
Higher Education Press

内容简介

本书作为信息安全专业教学的专业课教材，有别于此前一些关于信息系统安全方面的书籍，不仅侧重于通信保密或计算机安全方面的内容，而且针对与计算机网络系统有关的开放系统互连的安全问题，从安全体系、安全服务、安全机制和安全管理等方面全方位地讲述信息系统安全的基础理论和方法。

本书的重点在于给出信息系统安全的基础理论背景知识、信息系统安全体系结构、开放系统互连安全框架及其机制的相关技术、系统安全技术和基本知识。在系统安全技术方面，对信息系统的入侵与攻击技术、防火墙技术、入侵检测与监控技术、物理隔离技术以及防病毒技术等主要内容进行了详细的讲解，并给出了一部分具体的运用方案。本书通过对信息系统安全的五大安全服务和多种实现机制给出比较完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

本书是针对计算机、通信、信息安全等专业本科和硕士研究生的教学特点，更加强调理论和工程技术应用相结合而编写的教材，同时也可供从事相关专业教学、科研和工程技术的人员参考。

图书在版编目(CIP)数据

信息系统安全理论与技术/方勇主编;刘嘉勇等编著.
2版.—北京:高等教育出版社,2008.3
ISBN 978-7-04-023349-0

Ⅰ.信… Ⅱ.①方…②刘… Ⅲ.信息系统-安全技术-高等学校-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2008)第 016697 号

出版发行	高等教育出版社	购书热线	010-58581118
社　　址	北京市西城区德外大街 4 号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京北苑印刷有限责任公司	畅想教育	http://www.widedu.com
		版　　次	2004 年 6 月第 1 版
开　　本	787×1092　1/16		2008 年 3 月第 2 版
印　　张	24	印　　次	2008 年 3 月第 1 次印刷
字　　数	540 000	定　　价	29.90 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　23349-00

第 2 版前言

《信息系统安全理论与技术（第 2 版）》一书是针对计算机、通信、信息安全等专业的本科和硕士研究生的教学特点而编写的教材，着重强调理论和工程技术应用的结合。

本书由 4 个部分构成。第一部分包括第 1 章，从信息系统和信息系统安全的层次结构引出信息系统安全的有关问题，并从信息系统风险控制点及其对抗措施和安全工程方法论方面为第二部分进行了必要的准备和铺垫。第二部分包括第 2 章、第 3 章，从信息系统安全体系的构建方法一直到安全框架、安全服务和安全机制进行了比较完整和系统的介绍，目的在于给出信息系统安全体系的架构和支持技术。第三部分包括第 4 章，重点介绍了信息系统安全风险评估的理论和技术。第 4 部分包括第 5 章、第 6 章、第 7 章、第 8 章、第 9 章和第 10 章，介绍了个人计算机安全配置和管理、网络黑客技术、防火墙技术、入侵与攻击技术、入侵检测与监控技术、防病毒技术、VPN 技术与安全 VPN 技术以及这些技术的实现方法。全书涉及的内容十分广泛，对于本科生、研究生的学习，可在内容、重点和深度方面根据学时数进行选择。

本书由四川大学信息安全研究所组织编写，戴宗坤教授对全书的体系结构和内容组织提出了宝贵的意见和建议，教育部高等学校信息安全类专业教学指导委员会秘书长方勇教授主审了全书，并提出很多宝贵意见，在此一并表示感谢。方勇编写第 1 章、第 2 章、第 3 章和第 6 章，胡勇编写第 4 章，欧晓聪编写第 5 章和第 9 章的部分内容，吴少华编写了第 9 章的第三节，刘嘉勇编写第 7 章和第 8 章，周安民编写第 10 章。关义章教授、何大可教授、李飞教授参与了本书内容编排的讨论。

四川大学信息安全研究所全体同志为本书的编写提供了优越的工作环境和多方面的帮助。此外，本书的编写也从其他老师和同行的著作（包括网站）中得到了帮助，在此一并表示衷心的感谢。

信息安全是一个新兴的、发展极为迅速的专业领域，本书涉及较多新的概念、内容和研究课题。由于作者水平有限，书中难免存在缺点和错误，诚望读者批评赐教，为推动我国信息系统安全工程高级技术人才的培养共同出力。

编者

2007 年 10 月 20 日

于四川大学信息安全研究所

第 1 版前言

本书是针对高等院校信息管理与信息系统、计算机、通信、信息安全等专业的本科和硕士研究生的教学特点，更加强调理论和工程技术应用相结合而编写的教材。

本书的重点在于给出信息系统安全的基础理论背景知识、信息系统安全体系结构、开放系统互连安全框架及其机制性技术、系统安全技术和基本知识。在系统安全技术方面，对信息系统的入侵与攻击技术、防火墙技术、入侵检测与监控技术、物理隔离技术以及防病毒技术的主要内容进行了介绍，并给出了一部分具体的运用方案。本书尤其通过对信息系统安全的五大安全服务和多种实现机制给出较为完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

本书由两个部分构成。第一部分包括第 1 章，从信息系统和信息系统安全的层次结构引出信息系统安全的有关问题，并从信息系统风险控制点及其对抗措施梗概和安全工程方法论方面为第二部分进行了必要的准备和铺垫。第二部分包括第 2 ~ 6 章，从信息系统安全体系的构建方法一直到安全框架、安全服务和安全机制进行了较为详细的介绍，比较完整和系统。本书的目的在于为读者提供信息系统安全体系的架构及支持技术，并重点讨论了防火墙技术、入侵检测与漏洞扫描技术、物理隔离技术，同时对恶意程序与病毒对计算机及网络系统的威胁及其对策以及技术实现方法进行了讲解，并对 PKI 做了比较详细的介绍。全书涉及的内容十分广泛，本科生或研究生在学习时，可根据学时数在内容、重点和深度方面进行选择。

本书由四川大学信息安全研究所组织编写，戴宗坤教授做了全书的结构设计和统筹，戴宗坤和罗万伯教授对全书进行了审校。方勇编写第 1、4、6 章和第 5 章的 5.3 节，其余部分由刘嘉勇编写。

四川大学信息安全研究所全体同志为本书的编写提供了优越的工作环境和多方面的帮助。本书的编写还从其他同行的著作（包括网站）中得到了帮助，在此一并表示衷心的感谢。

目　录

第1章

绪　论

本章基于信息系统的基本概念，描述了信息系统安全的内涵和方法论；指出了信息系统存在的风险、信息系统的安全需求以及信息系统常见的威胁和防御策略；阐述了信息系统的安全要素。

1.1　信息系统概述

1.1.1　信息系统的定义

所谓系统，是指由相互联系、相互作用又相互依存的若干单元组成的、具有一个共同目标的有机整体。从数学角度看，系统又是具有某一或某些共同属性的元素的集合。

关于信息系统的概念，存在多种定义，比较流行的定义有以下几种：

①《大英百科全书》的解释：信息系统是有目的、和谐地处理信息的主要工具，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。

② M. 巴克兰德（M. Buckland）的定义：信息系统是提供信息服务，使人们获取信息的系统。

③ N. M. 达菲（N. M. Dafe）等的定义：信息系统大体上是人员、过程、数据的集合，有时也包括硬件和软件。它收集、处理、存储和传递在业务层次上的事务处理数据并支持管理决策的信息。

④ 中国学者吴民伟的定义：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。信息系统要利用计算机硬件、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，对信息系统的定义是同中有异，异中有同。但是，如果将信息系统涉及的功能与范围加以适当界定，可大体统一为两种定义。广义的信息系统包括的范围很广，各种处理信息系统都可称为信息系统，包括人体本身和各种人造系统；狭义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备、工具的有机集合，它突出的是计算机、网络通信、信息处理等技术的应用。本书所研究的内容将信息系统划在后一种定义的范畴。

1.1.2 信息系统的发展过程

从概念上讲，信息系统在计算机问世之前就已存在。自20世纪初泰罗创立科学管理理论以后，管理科学与方法、技术得到迅速发展；在它与统计理论和方法、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，在近半个世纪以来得到迅猛发展。信息系统的发展经历了以下阶段：

1. 电子数据处理系统阶段

电子数据处理系统（Electronic Data Processing System，EDPS）是用计算机模仿手工管理方式，进行事务性数据处理的系统，因此也将其称为事务处理系统（Transaction Processing System，TPS）。这一阶段从20世纪60年代初开始，用计算机计算工资、打印报表等。电子数据处理系统存在一些缺陷，局部模拟了人工系统，受限于当时计算机的能力和人们对计算机的认知，数据收集速度慢且容易出错等成为该系统最薄弱的环节。

2. 管理信息系统阶段

管理信息系统（Management Information System，MIS）是在事务处理系统基础上发展起来的第二代信息系统，两者有显著的区别：事务处理系统处理和获取数据，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，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。

3. 决策支持系统阶段和专家系统

决策支持系统（Decision Support System，DSS）是面向半结构化决策问题，支持中高级决策者决策活动的人－机信息系统，是辅助决策工作的一种信息系统，其特点是重点在“支持”而非决策工作的自动化。

专家系统（Expert System，ES）就是一个具有智能特点的计算机程序，它的智能化主要表现为能够在特定的领域内模仿人类专家思维来求解复杂问题。因此，专家系统必须包含领域专家的大量知识，拥有类似人类专家思维的推理能力，并能用这些知识来解决实际问题。

4. 办公自动化系统阶段和多媒体信息系统

严格说来，办公自动化系统（Office Automation System，OAS）/多媒体信息系统（Multimedia Information System，MMIS）是电子数据处理系统（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，并不是新型的信息系统。但是，正是办公自动化系统在20世纪80年代的广泛应用、多媒体信息系统在20世纪90年代的兴起，才使信息系统这一领域更加引人注目，而多媒体信息系统自身也成为各类信息系统应用的方向。

信息系统各阶段的类型、特点如表1－1所示。

表 1-1 信息系统各阶段的类型及其特点

阶段	类型	特 点
1	数据处理系统	完成机械任务
2	事务处理系统	用计算机代替手工程序
3	管理信息系统	提供用于管理决策过程的信息
4	决策支持系统	为决策提供信息，并成为实际决策过程的一个组成部分

1.2 信息系统安全

1.2.1 基本概念

信息系统安全是指信息系统的安全，而非信息的系统安全。当人们谈及与计算机网络（或 Internet）有关的信息系统的安全时，往往说成是信息安全。一般而言，信息安全与信息系统安全是安全集与安全子集的关系，具有包含与被包含的关系。信息安全有着更广泛、更普遍的意义，涵盖了人工和自动信息处理的安全以及网络化与非网络化的信息系统安全，泛指一切以声、光、电信号、磁信号、语音以及约定形式等为载体的信息的安全，一般也包含以纸介质、磁介质、胶片、有线信道以及无线信道为媒体的信息，在获取（包括信息转换）、分类、排序、检索、传递和共享时的安全。

在本书中，将信息系统安全定义为：确保以电磁信号为主要形式的、在计算机网络化（开放互连）系统中进行自动通信、处理和利用的信息内容，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，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。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、网络互连设备、传输介质、信息内容及其操作系统、通信协议和应用程序所构成的物理的和逻辑的完整体系；环境则是系统稳定和可靠运行所需要的保障体系，包括建筑物、机房、动力保障与备份以及应急与恢复体系。

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，它研究如何建立信息系统的数学模型，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试验设计方法。

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。这种特定状态就是信息系统处于动态平衡的状态。因此，调整的方向和目标就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）。

上述定义源于两种研究方法，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信息系统安全稳定在某一可控的特定状态内。

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唯一和最终的目标是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，但是离开了信息系统安全的体系，孤立地和单纯地去寻求直接保护信息内容的方法，显然是不合理的。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。为此，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，有必要从方法论的角度去理解和构造信息系统安全体系或模式。

信息系统安全方法的要点包括：

① 信息系统是一项系统工程，由信息系统功能性工程和确保信息系统按照管理者要求可靠、稳定、有序地实现其功能的安全性工程有机地结合起来。

② 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。

③ 信息系统功能性工程各组件要素，在实现系统功能的过程中应确保信息内容的机密性、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，可能遭遇的来自系统内部和外部的对系统的骚扰、入侵以及对信息的窃听、截获、注入和修改等威胁和攻击。

④ 针对上述问题，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，恰当地采用各种安全技术机制在相应的信息系统功能性工程各组件要素上构建安全框架，直接或间接提供必要的安全服务。

显然，信息系统安全性工程是一个嵌入功能性工程中的控制体系，是功能性工程的保障体系。这里需要特别强调两个问题，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备和实体，也可以是虚化的设备和实体；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。

1.2.2 信息保密与信息系统安全

就信息安全和信息系统安全而言，保证信息（内容）的保（机）密性是信息系统安全的基本目标之一。从信息保密性角度来看，信息（系统）安全涵盖了信息保密的内容。但是，

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，与一般意义上信息安全中的机密性相比，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等特点，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等特点。

在强调信息系统安全和保密时，是将保密作为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。作为安全策略，保密还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控制等。显然，作为安全策略，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。

1.3 影响信息系统安全的因素

所谓信息系统的风险是对某个脆弱性可能引发某种成功攻击的可能性及其危害性的测度。当某个脆弱的资源价值越高，受到成功攻击的概率越大时，风险也就越高；反之，当某个脆弱的资源价值越低，受到成功攻击的概率越小时，风险也就越低。风险分析是信息系统安全需求分析的依据，通过风险分析可明确风险的类型及其影响范围，使信息系统针对可能的风险采取相应的防护措施。

信息系统的风险分析可分为3个层次：

① 信息系统静态风险分析。在信息系统设计和运行前，对其可能面临的风险进行分析，分析信息系统存在的薄弱点，易于受到攻击的点或范围，并界定信息系统最宽松的安全边界。

② 信息系统动态风险分析。在信息系统运行过程中进行测试，跟踪并记录其有关活动，以发现信息系统运行期新出现的风险或原有风险的变化情况。

③ 信息系统运行后的风险分析。提供相应的信息系统风险分析报告。

风险分析是信息系统安全需求的依据，安全需求则是制定和实施安全策略的依据。对一个完整体系的信息系统安全来说，由于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的和空间分布的。一般而言，由于人们对风险有一个认识过程，安全需求总是滞后于风险的发生和发展。但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，建立起具有自适应能力的信息安全模型，从而驾驭风险，将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，零风险永远是一个可期而不可达的目标，因此信息系统安全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。

1.3.1 信息系统自身的安全脆弱性

由于自身主体和客体的原因，信息系统可能存在不同程度的脆弱性，从而为各种攻击提供了可利用的途径和方法。所谓信息系统的脆弱性，是指信息系统的硬件资源、通信资源、软件及信息资源等因可预见或不可预见甚至恶意的原因而可能导致信息系统受到破坏、更改、泄露和功能失效，从而使信息系统处于异常状态甚至崩溃、瘫痪等的根源和起因。

1. 硬件组件

信息系统硬件组件的安全隐患多来源于设计，主要表现为物理安全方面的问题。例如，各种计算机或网络设备（如主机、CRT、电缆、HUB、路由器、微波线路等），除难以抗拒的自然灾害外，温度、湿度、尘埃、静电、电磁场等也可以造成信息的泄露或失效。信息系统在工作时向外辐射电磁波，易造成敏感信息的泄漏。由于这些问题是固有的，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，因此在设计硬件和选购硬件时应尽可能减少或消除此类安全隐患。

2. 软件组件

软件组件的安全隐患来源于设计和软件工程中的问题。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，不可避免地会引起安全脆弱性；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预期；软件工程实现中造成的软件系统内部逻辑混乱，导致出现垃圾软件，这种软件从安全角度看是绝对不可用的。

软件组件可分为3种类别，即操作平台软件、应用平台软件和应用业务软件。这三类软件以层次结构构成软件组件体系。

操作平台软件处于基础层，维系着信息系统组件运行的平台。操作平台软件的任何风险都可能直接危及或被转移、延伸到应用平台软件，因此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，强烈建议安全服务组件的操作系统不得直接采用商业级或普遍使用的操作系统。

应用平台软件处于中间层次，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，其任何风险可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也至关重要，在提供自身安全保护的同时，还必须为应用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，因为它不能直

接与异构网络进行连接和通信。这样的“封闭”网络本身基于两个原因，比开放式的 Internet 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信息系统的可能性，但信息的电磁泄露性和基于协议分析的搭线截获问题仍然存在；二是专用网络自身具有比较完善、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 协议的 Internet 及其通信协议。因为任何接入 Internet 的计算机网络以及利用公共通信基础设施构建的内联网/外联网，无论在理论上还是技术实践上已无真正的物理界限，同时在地缘上也没有真正的国界，国与国之间、组织与组织之间以及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，因此 Internet 是一种虚拟的网络现实；支持 Internet 运行的 TCP/IP 协议原本只考虑了互连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中的大量安全问题。要理解与 Internet 有关的安全脆弱性、漏洞存在的原因和分布情况，需要从网络技术发展史和 TCP/IP 协议的研究初衷、使用背景以及发展驱动力等方面进行分析。

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）”的扩张模式。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，并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。而作为公共基础通信设备的网络则使用 X.25、FR、ISDN、DDN、PSTN 等交换技术，信息访问的存取方式主要有主机方式和客户机/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，随后又陆续推出了相应的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多种商业利益的驱动，实际上迄今为止并没有真正的产品完全遵从这些标准，世界上的大多数网络使用的仍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，基本上使用的也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，内部通信和信息共享可以遵从各自体系的同一标准，而要在两种异构网络之间进行通信则困难很大，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。

消除这一技术屏障的研究一直在进行。获得成功的是美国国防部高级研究计划署（DARPA）于 1973 年启动的互联网计划。该计划原本用于解决军事部门内部各种计算机网络的互连问题，其互连的网络被称为 Internet DARPA。为此，美国军方组织了包括美国大学、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，开发了用于 Internet 的 TCP/IP 协议。这项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 4 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 月将其移交给当时的美国国防通信局（DCA）进行控制和管理。在此基础上，组建了 ARPA Internet，美国国防通信局要求所有互联的网络都使用 TCP/IP 协议。1986 年，ARPAnet 正式分为两大部分，即美国国家基金会（NSF）资助的 NSFnet 和军方独立的国防数据网 MILnet。由于美国国家基金会的支持，许多地区和院校的网络开始使用 TCP/IP 协议和 NSFnet 连接，Internet 的名字作为使用 TCP/IP 协议连接的各个网络

的总称被正式采用。美国国家科学基金会在1990年制定的可接受的使用策略（Acceptable Use Policy），促进了Internet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技术扩大到用于提供到世界许多地方的连接服务。此后，一些大的网络公司认识到Internet的巨大商业价值，它们推动美国政府建立了国家信息基础设备（NII），即所谓信息高速公路的建设。

基于TCP/IP协议的Internet技术的发展极为成功，其主要原因是它使用了统一的、有效用于网络互连的网络通信协议TCP/IP，并被开发为适用于各种软件的平台，从而打破了异型计算机之间、异构网络之间互连互通的技术屏障；利用TCP/IP技术开发的各种各样的服务软件，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和个人用户；Internet采用了主干地区、园区的分层网络互连结构，其用户覆盖面极大，具有网络用户扩展的物理空间。以上3个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，充分调动了参与者的积极性，使人类仅用了几年的时间就创造了一个全球互联网（Internet）。

人们在享受Internet技术给全球信息共享带来的方便性和灵活性的同时，已经认识到基于TCP/IP的Internet是在可信任网络环境中开发出来的成果，主要体现在TCP/IP协议上的总体构想和设计本身，基本未考虑安全问题，并不提供人们所需的安全性和保密性。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，就发生了信任问题。因此，就不难理解Internet充满了安全隐患。概括起来，Internet体系存在着以下几种致命的安全隐患：

（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地址作为网络结点的唯一标识，而IP地址的使用和管理又存在很多问题，因此可导致两种主要的安全隐患：

① IP地址是由Internet信息中心（InterNIC）分发的，其数据包的源地址很容易被发现，且IP地址隐含了所使用的子网掩码，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Internet来说是暴露的。

② IP地址很容易被伪造和更改，且TCP/IP协议无针对IP包中源地址真实性的鉴别机制和保密机制，因此Internet上任何主机都可以产生一个带有任意源IP地址的IP包，从而假冒另一台主机进行地址欺骗。

（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，对路由信息缺乏鉴别与保护，因此可以通过Internet利用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协议规定了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，除了可能面临IP层所遇到的安全威胁以外，还存在TCP/UDP实现中的安全隐患：