信息系统安全理论与技术

蔡　勉　卫宏儒　主编

北京工业大学出版社

内 容 摘 要

信息资源是社会发展中很重要的战略资源。随着对信息化依赖程度的增加，信息安全问题就凸现出来，如不采取有效的对策将对信息安全产生重大不利影响，并严重威胁国计民生及社会的稳定和发展。信息安全涉及安全政策、安全技术、安全管理、安全产业、信息安全基本设施和信息安全有效评估等方面。本书阐述了信息安全的基本概念、原理、安全标准，并针对局域网、无线局域网、移动通信系统提出了如何建立安全体系和必要的防护措施。

本书内容编排合理，结构清晰，循序渐进，通俗易懂，可作为高等院校计算机及其相关专业的信息安全课程教材，也可供相关技术人员阅读参考。

图书在版编目（CIP）数据

信息系统安全理论与技术/蔡勉，卫宏儒主编 .—北京：北京工业大学出版社，2006.9

ISBN 7-5639-1634-2

Ⅰ.信 … Ⅱ.①蔡 …②卫 … 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（2006）第 005549 号

信息系统安全理论与技术

蔡勉 卫宏儒 主编

*

北京工业大学出版社出版发行

邮编：100022 电话：（010）67392308

各地新华书店经销

徐水宏远印刷厂印刷

*

2006 年 9 月第 1 版 2006 年 9 月第 1 次印刷

787 mm×1 092 mm 16 开本 20.75 印张 512 千字

印数：1～3 000 册

ISBN 7-5639-1634-2/T·278

定价：32.00 元

前　言

信息资源是社会发展中重要的战略资源，信息化程度也是国家现代化水平和综合国力的重要标志。信息网络的社会化和国际化使信息版图不断扩展，信息化已深入到我国政治、军事、经济、社会、企业、生活等多种领域。以互联网为代表的信息基础设施对国家、地区、企业、部门、家庭的信息化进程产生了重大影响。随着对信息化依赖程度的增加，信息安全问题就凸现出来，计算机黑客的猖獗、计算机病毒的泛滥、有害内容的恶性传播、国际信息间谍的潜入、网络恐怖活动的威胁、信息战争的阴影等网络攻击和犯罪呈明显上升的趋势，如不采取有效的对策将对信息安全产生重大不利影响，并严重威胁国计民生及社会的稳定和发展。重视信息安全已成为我国政府和社会普遍关注的焦点，研究信息安全面临的安全政策、安全技术、安全管理、安全产业、信息安全基础设施等问题和信息安全的有效评估问题，是摆在我们面前的重要任务。

本书共分为两大部分。第 1～6 章是第一部分，主要是信息系统安全的理论部分。其中：

第 1 章重点讲述了我国发展信息安全的意义，即信息安全的发展趋势和需要解决的问题。

第 2 章重点讲述了密码学的相关概念。密码学是研究密码系统和通信安全保密的学科，它是研究信息系统安全的理论基础。

第 3 章讲述的是与密码学相关的数学知识。

第 4 章重点讲述流密码。流密码是密码学的一个重要分支，人们对它的研究比较充分，并且有比较成熟的数学理论支持。流密码具有软件实现简单、便于硬件实现、速度快和效率高的特点。目前，流密码是世界各国的军事和外交等领域使用的主要密码体制之一，也是新一代移动通信的主流加密算法。

第 5 章讲述分组密码。它在通信网络（尤其是计算机通信）和系统安全领域有着广泛而重要的应用。

第 6 章讲述公钥密码体制。它既能用计算机来进行高速加解密，又能使密钥通用，且在不换密钥的情况下密钥仍可反复使用，而不会被密码分析者破译，目前在政府网、VPN、电子商务等领域内都比较流行。

第 7～14 章是第二部分，这一部分主要讲述的是信息系统安全的技术层面。其中：

第 7 章讲述数字签名。数字签名是电子商务安全的一个非常重要的分支，是实现电子交易安全的核心技术之一。它在实现身份认证、数据完整性、不可否认等功能方面都有重要的应用，尤其在大型网络安全通信中的密钥分配、公文安全传输以及电子商务和电子政务等方面有重要应用价值。

第 8 章讲述身份证明。主要讨论几种可能的技术，如口令认证系统、个人特征的身份证明以及 X.509 证书系统等。

第 9 章讲述安全协议。

第 10 章讲述网络安全技术，主要内容为计算机病毒及其防范、防火墙技术、入侵检测技术、访问控制技术的原理及应用。

第 11 章讲述无线局域网安全。无线网络的安全问题是制约无线网络技术发展的“软肋”，由于无线网络的传输具有开放性，所以它受攻击的可能性比有线网络更大。本章主要讨论无线局域网安全标准，主要涉及无线局域网系统的安全结构、安全机制和实现安全策略的各种途径和方案。

第 12 章讲述信息安全技术。主要阐述了信息隐藏技术、电子支付技术、智能卡安全技术的相关知识。

第 13 章讲述移动通信系统安全。

第 14 章讲述信息系统安全评估。目前，研究信息安全面临的安全政策、安全技术、安全管理、安全产业、信息安全基础设施等问题和信息安全的有效评估问题，是摆在我们面前的重要任务。本章主要就信息系统评估的相关知识作一介绍。

在本书的编写过程中，北京工业大学的研究生王建明、孙兴芳、倪海东、金怡等参与了录入、编辑、资料收集和整理工作，康莉、李梅娟、茹斌等参与了校订工作；同时同行的著作对我们也大有帮助，在此表示感谢。

由于水平有限，书中难免会出现一些错误，敬请读者批评指正，以便今后对此书进行修订和完善。

编　者

2006 年 6 月

目　录

第1章 绪 论

随着传统的资源经济在全世界范围内大规模地向知识经济转变，人类社会也在全方位地接受着信息化的洗礼。特别是步入20世纪90年代之后，高速信息传输网络的建设，将人们带进了一个极具魅力和活力的网络环境，也在社会信息化的进程中树立了一座新的里程碑。高速信息传输网络是一个遍布各地的、易于使用的、安全的、多功能的、信息丰富的和开放的系统，从技术的角度看，它是现代信息技术不断发展与集成的结果。

在高度发达的信息社会，信息已成为一种社会资源，它被看做是与材料和能源同等重要的、支持社会发展的三大支柱之一，对现代社会的生存和发展有着重要作用。作为信息传输媒体的信息系统已经成为一个国家、一个行业、一个企业或一个集团寻求发展的基础设施。计算机网络是信息传播的平台，构成了网络信息系统的基础。由于信息网络具有国际化、社会化、开放化、个人化的特点，从而给人类带来了巨大的益处，例如缩小了人们彼此间的空间，缩短了信息传输时间，共享信息资源，这些都强有力地促进了人类社会的发展。人类在感受网络信息系统对社会文明的巨大贡献的同时，也认识到网络信息安全问题已成为影响国家、企业大局和长远利益而亟待解决的重大关键问题。随着人们对信息化依赖程度的增加，计算机黑客的猖獗、计算机病毒的泛滥、有害内容的恶性传播、国际信息间谍的潜入、网络恐怖活动的威胁以及信息战争的阴影等网络攻击和犯罪呈明显上升的趋势，如不采取有效对策将产生重大后患，面临巨大的风险。对国家而言，没有网络安全解决方案，就没有信息基础设施的安全保证，就没有网络空间上的国家主权和国家安全，国家的政治、军事、经济、文化、社会生活等将处于信息战的威胁之中。因此，必须加强信息安全保障工作，全面提高信息安全防护能力，创建安全健康的网络环境，从而保障和促进信息化发展，保护公众利益，维护国家安全，构筑国家信息安全保障体系。同样，信息系统安全关系到企业的生存与发展。

近些年，我国在信息安全方面也做了很多工作。2000年，科技部启动了“863信息安全应急计划”——成立了国家信息安全发展战略研究专家组，全面部署和宏观统筹信息安全工作；在四川成都、湖北武汉和上海，建立了信息安全成果产业化的西部、中部和东部基地；组建了三家信息安全研究中心和教育培训中心，加强自主开发和创新能力；在上海实施国家信息安全应用示范工程（S219）。经过近三年的努力，信息安全产业化基地、研究和教育培训中心、S219工程的建设都取得了重大突破。

信息系统安全是一个综合性的学科，它涉及数学、密码学、计算机、通信、控制、人工智能、安全工程、人文科学等诸多学科，是近几年迅速发展的一个热点学科。

1.1 信息技术与信息系统

1.1.1 信息技术的概念

人类对信息的应用已有数千年的历史，人类信息活动的演进与信息技术的发展是密不可分的。可以说，人类信息活动的每次演进都会引起信息技术的革命性变化，而信息技术的每次发展同样会促进人类信息能力的提高。

信息技术是一个含义广泛、复杂而又时刻变化着的概念。所谓信息技术，大而言之，是指应用信息科学的原理和方法同信息打交道的技术；小而言之，是指有关信息产生、检测、变换、存储、传递、处理、显示、识别、提取、再生、控制和利用等的技术。

20世纪40年代以来，从最具创造力的电子计算机的问世，到已渗入人类生活方方面面的高速信息传输网络的建设，信息技术得到了空前的发展。现代信息技术的综合性很强，它包括的单元技术十分广泛，但从根本上看，它主要以微电子技术为基础，以电子计算机技术和通信技术为主要标志。

微电子技术是实现信息高速传递和交换的一种良好手段，是信息技术发展的重要基础。微电子技术与信息技术结合产生出一门重要的技术即电子信息技术。微电子技术也是其他高科技的基础，它渗透力最强，影响面最广，可以应用于生产、生活、科研等领域的诸多方面。

电子计算机技术既是现代信息技术的开端，也是现代信息技术的核心。计算机的出现从根本上改变了人类处理信息的手段，突破了人类大脑及感觉器官加工处理信息的局限性，人类借助计算机辅助人脑而有效地加工处理信息。

通信技术的飞速发展为迅速、准确、有效地传输信息提供了坚实的基础。特别是计算机与通信的结合，不仅使现代通信系统在计算机的控制下实现了传输的自动化和高效化，使各种通信方式一体化，而且使计算机借助通信线路实现了网络化，同时也使信息技术进入了信息传输、处理、存储综合化的新境界。

1.1.2 信息技术的特点

(1) 信息具有不灭性。信息的不灭性是指一条信息产生后，其载体可以变换，可以被毁掉，如一本书、一张光盘，但信息本身并没有被消灭。所以，信息的不灭性是信息的一个很大的特点。

(2) 信息可以廉价复制，可以广泛传播。把一条信息复制成一百万条信息的费用十分低廉。尽管信息的创造可能需要很大的投入，但复制只需要载体的成本。

(3) 某些信息的价值有很强的时效性。一条信息在某一时刻价值非常高，但过了这一时刻，可能一点价值也没有。现在的金融信息，在需要知道时，会非常有价值，但过了这一时刻，就会毫无价值。又如战争时的信息，敌方的信息在某一时刻有非常重要的价值，可以决定战争的胜负，但过了这一时刻，信息就变得毫无用处。所以说，相当一部分信息有非常强

的时效性。

1.1.3 信息技术对社会发展的影响

信息技术对人类社会的影响是广泛而深刻的。现代信息技术的最显著成就是建立了不断完善的面向全社会的信息网络，它与信息社会的生产力水平相对应。现代信息技术在高技术群体中居于先导与核心地位，并已成为当今世界发展科学技术、提高生产力、繁荣经济和发展社会的巨大力量。

信息技术的发展不仅影响经济的发展，而且在企业管理、生活、文化、科学研究、人类思维和政治领域都产生了深远的影响。

(1) 对经济的影响。信息技术的发展使生产要素得到了优化配置与合理流动，形成了劳动者操作的知识化和间接化；使传统产业得到改造，减少了物质资源和能源的消耗，环境污染等弊病将随之减少。

(2) 对企业管理的影响。信息技术促使管理者和被管理者不断更新管理思想，提高素质；使高层决策者与基层执行者可直接进行信息交流，使得管理结构由金字塔型变为矩阵型；同时有助于管理方法的完善，以适应虚拟办公、电子商务、软式制造、即时生产等新的运作方式，从而增强管理功能，加强管理的科学化和民主化，促进管理业务的合理重组。

(3) 对科学研究的影响。信息技术有利于科学研究前期工作的顺利开展，检索学术信息的范围和线索更全更广，通过电子邮件、线上交谈更便于与同行、跨行业专家交流；并且提高了科研工作效率，通过计算机可以快速完成大规模的数据处理。

(4) 对文化的影响。信息技术使文化更加开放，进而促进了不同国度、不同民族之间的文化碰撞与交流、学习与借鉴；信息技术还使文化更加大众化，人们可以方便地在网上发表文学作品，利用网上图书馆和博物馆等。

(5) 对思维的影响。信息技术的进步促进了人们思维方式的科学化、现代化、多元化，以及创造性、前瞻性、灵活性，人们对信息的大量和快速摄取，将不断促进人类思想产生新的见解、新的发现、新的突破。

(6) 对生活的影响。电子购物、电子金融、电子邮政、电子书刊、电子娱乐、远程医疗、远程教育等丰富多彩的服务项目使人们足不出户而尽为天下事，人们的生活中心将发生空前转移，从原来的社会转向家庭，使家庭成为人们生活的新中心。

(7) 对政府的影响。信息技术从技术手段上强化了国家功能，可为政府的科学决策提供实时、全面、可靠的数据和信息依据，大大降低了决策的不确定性和盲目性；可使各部门及时沟通和协调，以利于政府直接、及时、有效地指导、管理、控制、监督，提高国家宏观调控的能力和效率。

信息技术的飞速发展，有力地促进了社会经济的发展，但是也存在一些负面影响。

(1) 信息爆炸。这是一个名副其实的“信息爆炸”时代，美国的一项新研究结果可以为证：加利福尼亚大学伯克利分校的研究人员发现，仅过去三年中，全球新生产的信息量就翻了一番。信息量加大的同时，也导致大量垃圾信息的产生，如何清理这些信息垃圾是个很大的难题。

(2) 信息犯罪。信息犯罪越来越严重，小到磁卡的伪造，大到金融系统的信息犯罪以及黑客犯罪等，已成为不可忽视的问题。例如，利用计算机网络进行色情活动，搞经济诈骗，

窃取银行资金，使他人系统失灵而导致机构运转瘫痪，甚至在网络上传授组装危险武器的知识等。通过计算机网络，还能够比较容易地获取和使用他人计算机中的信息，一些别有用心之人则可通过计算机网络窃取个人、企业、机构和政府的商业、军事、政治机密，造成信息失窃，甚至威胁国家的安全。

(3) 信息病毒。计算机病毒给整个信息网络，乃至整个社会带来的危害是无法估量的。据报道，世界上大约有几千种计算机病毒在传播流行，同时每天又有 5～10 种新病毒在不断地产生和蔓延。它们轻则降低计算机运行速度和效率，重则能够销毁系统中的所有数据、删除文件、对磁盘进行格式化等。编制、设计各种计算机病毒不仅造成了信息利用障碍，而且在信息技术领域刮起了恐怖风暴。据报道，计算机黑客每年给全世界网络带来 100 亿美元的损失。

(4) 信息渗透。信息渗透是指西方发达国家在向第三世界输出影视作品、广告、艺术品、网络信息的同时，也在潜移默化地输出他们的生活方式、伦理道德、文化观念和行为规则。在这种情况下，各民族文化的独特性和差异性受到了挑战，一些古老的风俗、纯朴的生活方式、社会理想等民族文化有被瓦解的可能。

(5) 信息安全保密问题。安全保密问题涉及很多方面，包括国家机密、企业机密、个人机密等。在安全方面，除了军事安全外，经济安全也是一个很大的问题，在当今技术条件下，几秒内可以把上亿的资产从一个地方转移到另一个地方，这是相当危险的。全球一天的金融交易量达到 1 万多亿美元，而全世界货物的实物交易量一年还不到 10 万亿美元。所以说，金融安全问题是一个非常大的问题，而其基础就是信息技术的安全性。

所以，在发展信息技术的同时，也要解决信息的安全性问题，这样才能使信息技术更好地为社会发展服务。

1.1.4 信息系统

信息系统是与“信息”有关的“系统”，就像“信息”、“系统”的定义具有多样性一样，人们对其定义也远未达成共识。在这里我们给出信息系统的定义是“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”。

与网络协议中的七层结构相似，信息系统也有自己的七层结构，如表 1-1 所示。

表 1-1 信息系统的七层结构

层 号	名 称	说 明	层 号	名 称	说 明
1	用户层	用户面向对象操作	5	工具层	信息系统开发工具
2	业务层	信息系统业务模型	6	OS 层	网络操作系统
3	功能层	信息系统功能模型	7	物理层	网络与通信硬件
4	数据层	信息系统数据模型	—	—	—

1. 工作机制

信息系统七层结构从宏观上揭开了信息系统的内部“秘密”，从微观上给设计者、实现者和用户指明了新的航向。

工具层、OS 层、物理层 3 层的有机组合与合理配置，属于系统硬件与系统软件的集成问题，是多数系统集成商所能胜任的工作，也是系统集成中最容易做的事情。它是整个信息

系统集成的物质基础。

数据层的最高目标是实现数据集成，它是信息系统集成的核心，是系统集成的重点和难点，是多数系统集成商想干而不敢干或不能干的事情。实现数据集成的方法是采用面向数据而不是采用面向功能的设计方法。

只要企业单位的业务方向和业务内容不变，其元数据（metadata）就是稳定的，而对元数据的处理是可变的。用不变的元数据对付可变的处理方法，就是面向数据设计的基本原理。面向数据设计的实现方式是使用 CASE 工具，如 PowerDesigner 或 Designer 2000。它的关键技术是用 E-R 图来组织所有的元数据，产生信息系统的概念数据模型（CDM），然后，由 CASE 工具自动将概念数据模型转化为物理数据模型（PDM）。

物理数据模型生成后，就可以用工具层中面向对象的开发工具，设计并实现功能模型中的各种功能，如录入、删除、修改、统计、查询、报表等各种操作。每项功能对应相应的图标或窗口，用户根据业务层的业务模型，可以随心所欲地进行操作，轻松愉快地实现企业网上的各种需求。

信息系统的七层结构也揭示了信息系统建设的基本方法：系统分析是从第 1 层开始，由上向下直至第 7 层结束；而系统设计与实现是从第 7 层开始，由下向上直至第 1 层结束。由上向下的分析和由下向上的实现，就是七层结构的内部逻辑。作为开发信息系统的软件公司，主要工作是在第 3、4 层。第 4 层是面向数据设计，第 3 层是面向对象实现。只要这两层工作规范有序，信息系统的零维护理想就能逐步实现。

2. 需要探讨的几个问题

（1）在数据层中设计数据模型的方法，到底用面向数据的方法还是面向对象的方法？

在 CASE 工具出现前，人们用手工或其他 Office 工具来建立数据模型。在 CASE 工具出现后，人们开始用它来建立数据模型。工具虽然不一样，但目标却是一致的，都是为了在 DBMS 上建立稳定可靠的数据结构和相应的数据字典，与面向对象设计方法无关。建立数据模型的方法在面向对象方法提出前就已经存在了。在面向对象方法出现之前，建立数据模型的方法是在面向数据设计和面向功能设计中选择。因为面向功能设计不能构成稳定可靠的数据模型，当功能变更时模型跟着变更，给开发与维护带来了不便，因此这种方法很快就被淘汰。在数据层建立数据模型是信息系统设计的中心工作。这项工作以面向数据开始，到面向对象结束。这种观点必须坚持下去，绝对不能动摇，直到关系数据库管理系统完全退出历史舞台，面向对象数据库管理系统完全占领数据库市场为止。

（2）面向对象设计、面向对象编程、面向对象实现、分布式对象、多层结构、COM/DCOM、CORBA 等标准、部件（component）新生事物，到底在信息系统七层结构中的哪几层发挥作用？

它们主要是在第 3 层即功能层发挥作用。在 C/S 结构中，功能层的工作完全由客户机来实现，这样的客户机被称为胖客户机。当出现了 Web 浏览器和 Web 服务器后，Web 浏览器与数据库服务器形成三层或多层结构，客户机上的功能层工作向 Web 服务器或应用服务器上迁移，使得客户机上的工作量大大减少，并由胖变瘦，成为瘦客户机。客户机瘦了，服务器都胖了吗？不一定，因为服务器由通用走向了专用，出现了专干某一类事情的服务器，如通信服务器、OA 服务器、应用服务器、数据库服务器。只有明确了这个问题，信息系统的设计者与实现者在面向对象与中间件的炒作中，才不会头脑发热，迷失方向。

1.2 信息安全

信息安全包括信息的保密性以及信息的完整性、信息的可用性、信息的可控性、信息的不可否认性等，主要涉及密码技术、防火墙技术、入侵检测技术、网络安全、数据库和操作系统的安全、计算机病毒及其防治、信息安全标准、安全信息系统的安全评价、信息安全管理和公钥基础设施等几个方面内容。随着网络信息技术的不断发展与应用，网络与信息安全的内涵也在不断延伸。

信息安全是一个广泛和抽象的概念，人们一般把涉及计算机网络安全、计算机通信系统安全和 Internet 接入安全等与信息相关的安全，称为信息安全。但信息安全不代表任何具体的个体或系统与安全有关的问题，而是用来说明个体或系统的部分与安全有关的问题，更多的是一种概念性的东西。

1.2.1 密码技术和防火墙技术

现代社会对信息安全的需求大部分可以通过密码技术来实现。密码技术是信息安全技术中的核心技术。信息的安全性主要包括两个方面，即信息的保密性和信息的认证性。保密的目的是防止对手破译系统中的机密信息，认证的目的是验证信息的发送者是真的，而不是冒充的。验证信息的完整性，即验证信息在传输或存储过程中未被篡改、重放或延迟等。信息的保密性和信息的认证性是信息安全性的两个不同方面，认证不能自动地提供保密性，而保密也不能自然地提供认证功能。在用密码技术保护的现代信息系统的安全性主要取决于对密钥的保护，而不是依赖于对算法或硬件本身的保护，即密码算法的安全性完全寓于密钥之中。可见，密钥的保护和管理在数据系统安全中是极为重要的。人们目前特别关注的是密钥托管技术。

信息的保密性是信息安全性的一个重要方面。保密的目的是防止对手破译信息系统中的机密信息。加密是实现信息保密性的一种重要手段，就是使用数学方法来重新组织数据，使得除了合法的接收者外，任何其他人要想恢复原先的“消息”（将原先的消息称作“明文”）或读懂变化后的“消息”（将变化后的消息称作“密文”）是非常困难的，密文变换成明文的过程称作解密。

所谓加密算法就是对明文进行加密时所采用的一组规则，解密算法就是对密文进行解密时所采用的一组规则。加密算法和解密算法的操作通常都是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。根据加密密钥和解密密钥是否相同，可将现有的加密体制分为两种：一种是私钥或对称加密体制，这种体制的加密密钥和解密密钥相同，其典型代表是美国的数据加密标准（DES）；另一种是公钥或非对称加密体制，这种体制的加密密钥和解密密钥不相同并且从其中一个很难推出另一个，加密密钥可以公开，而解密密钥可由用户自己秘密保存，其典型代表是 RSA 体制。

信息的认证性是信息安全性的另一个重要方面。认证的目的有两个：一是验证信息的发送者是真的，而不是冒充的；二是验证信息的完整性，即验证信息在传输或存储过程中是否

被篡改、重放或延迟等。

对密码系统的攻击主要有两类：一类是被动攻击，对手只是对截获的密文进行分析；另一类是主动攻击，对手通过采用删除、增添、重放和伪造等手段主动向系统注入假消息。认证是防止他人对系统进行主动攻击（如伪造、篡改信息等）的一种重要技术。政治、军事、外交等活动中签署文件，商业上签订契约和合同以及日常生活中在书信、从银行取款等事务中的签字，传统上都采用手书签名或印鉴。签名起到认证、核准和生效的作用。随着信息时代的来临，人们希望通过数字通信网络进行远距离的贸易合同的签名，数字签名应运而生，并开始用于商业通信系统，如电子邮递、电子转账、办公室自动化等系统。

通信和数据系统的安全性常常取决于能否正确识别通信用户或终端的个人身份，比如银行的自动取款机（ATM）可将现款发放给经它正确识别的账号持卡人。对计算机的访问和使用、安全地区的出入和放行、出入境等都是以准确的身份识别为基础的。身份识别技术能使识别者让对方识别自己的真正身份，确保识别者的合法权益。但是从更深一层意义上来看，它是社会责任制的体现和社会管理的需要。

进入电子信息社会，虽然有不少学者试图使用电子化生物唯一识别信息（如指纹、掌纹、声纹、视网膜、脸形等），但由于代价高、准确性低、存储空间大和传输效率低，不适合计算机读取和判别，只能作为辅助措施应用。而使用密码技术，特别是公钥密码技术，能够设计出安全性高的识别协议，所以受到人们的青睐。

根据密码假设，一个密码系统的安全性取决于对密钥的保护，而不是对系统或硬件本身的保护。密钥的保密和安全管理在数据系统安全中是极为重要的。密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁等内容，其中密钥的分配和存储可能是最棘手的问题。密钥管理不仅影响系统的安全性，而且涉及系统的可靠性、有效性和经济性。当然，在密钥管理过程中也不可能避免物理上、人事上、规程上等一些问题。

防火墙是指设置在不同网络（如可信的企业内部网络和不可信的公共网络）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

从技术上讲，防火墙是一个系统或系统组，它在两个网络之间实施安全政策所要求的访问控制。它具有如下基本特点：所有的从内部通向外部或从外部通向内部的通信业务都必须经过它；能够根据安全政策提供需要的安全功能；只有经过授权的通信业务才允许通过它进出；系统自身对入侵是免疫的。

防火墙是网络安全的屏障，一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险；防火墙可以强化网络安全策略，通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上；对网络存取和访问进行监控审计，防火墙就能记录下访问并作出日志记录，同时也能提供网络使用情况的统计数据；防止内部信息的外泄，通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系：VPN。

防火墙技术可根据防范的方式和侧重点的不同而分为很多种类型，但总体来讲可分为两

大类：分组过滤、应用代理。分组过滤作用在网络层和传输层，它根据分组包头源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。应用代理作用在应用层，其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。复合型防火墙由于对更高安全性的要求，常把基于包过滤的方法与基于应用代理的方法结合起来，形成复合型防火墙产品。

1.2.2 入侵检测技术

随着个人、企业和政府机构日益依赖于 Internet 进行通信、协作及销售，对安全解决方案的需求急剧增长。这些安全解决方案应该能够阻止入侵者同时又能保证客户及合作伙伴的安全访问。虽然防火墙及强大的身份验证能够保护系统不受未经授权访问的侵扰，但是它们对专业黑客或恶意的经授权用户却无能为力。企业经常在防火墙系统上投入大量的资金，在 Internet 入口处部署防火墙系统来保证安全，依赖防火墙建立网络的组织往往是“外紧内松”，无法阻止内部人员所做的攻击，对信息流的控制缺乏灵活性，从外面看非常安全，但内部缺乏必要的安全措施。据统计，全球 80% 以上的入侵来自于内部。由于性能的限制，防火墙通常不能提供实时的入侵检测能力，对于企业内部人员所做的攻击，防火墙形同虚设。

入侵检测是指“通过对行为、安全日志或审计数据或其他网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图”（参见国家标准 GB/T 18336—2001）。入侵检测是检测和响应计算机误用的学科，其作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。进行入侵检测的软件与硬件的组合便是入侵检测系统（Intrusion Detection System，IDS）。

入侵检测是对防火墙极为有益的补充，入侵检测系统能使入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵者。在入侵攻击过程中，能减少入侵攻击所造成的损失。在被入侵攻击后，收集入侵攻击的相关信息，作为防范系统的知识，添加进知识库内，增强系统的防范能力，避免系统再次受到入侵。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监听，从而提供对内部攻击、外部攻击和误操作的实时保护，大大提高了网络的安全性。

1.2.3 网络安全

网络安全是信息安全的一个重要部分。以 Internet 为代表的信息网络技术的应用正日益普及，应用层次也在不断深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展。随着网络技术的普及应用，网络的安全成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求。网络安全已成为政府机构、企事业单位信息化所要考虑的重要问题之一。

建立在当今互联网技术基础上遍布世界各地的大大小小的网络信息系统，或多或少地存在着各种安全方面的隐患和漏洞。这些漏洞有的源于网络本身，有的源于系统本身，有的虽然采取了一些安全防护措施但是技术陈旧，抵挡不了外界的进攻，更多的则是由于应用和管理混乱甚至根本不设防。鉴于网络系统的复杂性和地域上的广泛性，今后可能会有更多的安