◎宁 葵 著

访问控制
Access Control

访问控制
安全技术及应用

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

访问控制安全技术及应用

宁 葵 著

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

内 容 简 介

访问控制技术是保证计算机安全最重要的核心技术之一，是维护计算机系统安全、保护计算机资源的重要手段。本书首先针对计算机访问控制技术做了一般性介绍，然后重点介绍其技术应用及安全产品，并对多款安全访问控制类产品的功能和性能进行了对比分析，对数码小卫士、加密金刚锁、虚拟保险箱、冰盾系统安全专家等软件的功能应用进行了描述，特别详细介绍了文件防弹衣单机版和网络版产品的使用，比较和总结了文件防弹衣的产品特点和优势，提出了构建文件防弹衣主动防御体系的新思路，阐明了计算机访问控制安全技术的发展方向。

本书适用于对访问控制防护技术以及网络安全技术感兴趣的读者，也可作为软件开发人员的产品设计的参考资料或技术人员的应用手册。

图书在版编目（CIP）数据

访问控制安全技术及应用 / 宁葵著. —北京：电子工业出版社，2005.10
ISBN 7-121-01833-0

Ⅰ. 访… Ⅱ. 宁… Ⅲ. 电子计算机－安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2005）第 118424 号

责任编辑：张燕虹
审　　校：于秀山
印　　刷：北京市天竺颖华印刷厂
出版发行：电子工业出版社
　　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：10.5　字数：240 千字
印　　次：2005 年 10 月第 1 次印刷
定　　价：16.80 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。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

网络技术的飞速发展，带来了全球信息资源与技术不可逆转的网络化发展趋势。网络技术对人类的影响是全方位、多层次的，以计算机网络技术为核心的计算机应用已广泛渗透到各个行业，成为影响科技、经济和文化发展的核心因素，并使社会的生产方式、工作方式乃至生活方式都发生了深刻变化。

然而，由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互连性等特征，致使其易受黑客、恶意软件和其他不轨行为的攻击，所以计算机信息的安全和保密是一个至关重要的问题。对于军用自动化网络、C^3I 系统和银行等传输敏感数据的计算机网络系统而言，其计算机信息的安全和保密尤为重要；无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素的脆弱性和潜在威胁。因此，计算机网络必须有足够强的安全措施，能全方位地针对各种不同的威胁和脆弱性，才能确保计算机信息的保密性、完整性和可用性。

访问控制技术是保证计算机安全最重要的核心技术之一，它是一种针对越权使用资源的防御措施，是计算机安全防范和保护的主要策略，它的主要任务是保证计算机资源不被非法使用和非法访问；同时，也是维护计算机系统安全、保护计算机资源的重要手段。

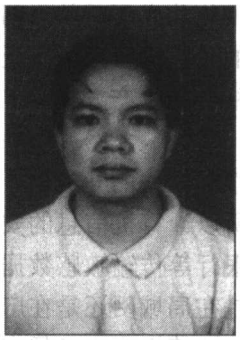
本书首先针对计算机访问控制技术做了一般性介绍，然后重点介绍了其技术应用和安全产品，并对多款安全访问控制类产品的功能和性能进行了对比分析。在编写过程中，我们以培养技术应用能力和职业素质教育为主线，力争打破以理论教学为本位、为目标、为标准的普通教育的教学模式，建立真正以培养技术应用型人才为目标的实践型教育教学模式，尽量避免理论内容过于追求系统性、完整性、严密性的现象，以及实践内容演示性多而实际操作少、高新技术含量低的现象，加强实训教学内容，大部分章节均设置介绍了技术与产品的实际应用，以强化技术应用能力的培养。本书力求思路清晰、结构合理、内容丰富、资料翔实，既反映和吸收本专业领域的最新进展，又融入我们自己的研究成果，使之具有较强的科学性、新颖性和实用性。

本书适用于对访问控制防护技术以及网络安全技术感兴趣的读者，也可作为软件开发人员的产品设计的参考资料或技术人员的应用手册。

限于认知和水准，书中可能存在疏漏和失当之处，敬请专家、学者及各位读者海涵斧正。

宁　葵

作 者 介 绍



宁葵，汉族，1970 年 4 月出生。1989 年 7 月于广西浦北中学高中毕业，1993 年获广西大学工学学士学位，2000 年于广西大学计算机应用研究生毕业。毕业后，一直从事计算机科学与技术领域的教学研究、技术研发、产品开发工作，主要研究方向有网络安全、分布式计算、软件工程等；发表的较典型的论文有“新一代的分布式计算技术——Web 服务”、“基于 OGSA 的网格系统研究”、“分布式拒绝服务攻击手段及其防范技术研究”、“一种基于角色访问控制的数据库安全模型”等，分别发表在《计算机工程》、《计算机与现代化》、《微机发展》等期刊上；是“文件防弹衣”项目的总负责人，该项目获 2004 年国家电子信息产业发展基金立项支持、2004 年广西科技厅立项支持、2003 年广西南宁市科技局立项支持、2004 年广西计算机推广应用成果一等奖、广西“优秀软件产品”等奖励。

目　录

第 1 章　计算机安全技术 …… 1

1.1　计算机安全技术概况 …… 1

1.1.1　计算机安全概述 …… 1

1.1.2　计算机信息安全策略 …… 2

1.1.3　计算机安全体系结构与模型 …… 3

1.2　计算机安全技术分类 …… 5

1.2.1　加密技术 …… 5

1.2.2　防火墙技术 …… 7

1.2.3　IDS（入侵检测技术） …… 9

1.2.4　病毒防范技术 …… 9

1.2.5　访问控制技术 …… 10

第 2 章　访问控制安全技术 …… 11

2.1　访问控制概述 …… 11

2.1.1　访问控制的起源 …… 11

2.1.2　访问控制的目标 …… 12

2.1.3　访问控制的要素 …… 13

2.1.4　访问控制的层次 …… 15

2.2　访问控制的分类 …… 17

2.2.1　自主访问控制 …… 17

2.2.2　强制访问控制 …… 19

2.2.3　基于角色的访问控制（RBAC） …… 20

2.2.4　类型裁决 …… 21

2.3　访问控制模型 …… 22

2.3.1　BLP 模型 …… 22

2.3.2　Biba 模型 …… 23

2.3.3　GM 模型 …… 23

2.3.4　Sutherland 模型 …… 24

2.3.5 CW 模型 …… 25
2.3.6 角色模型 …… 26
2.4 访问控制策略 …… 26
2.4.1 安全策略 …… 27
2.4.2 基于身份的安全策略 …… 28
2.4.3 基于规则的安全策略 …… 28
2.5 访问控制模型的实现 …… 29
2.5.1 访问控制模型的实现机制 …… 29
2.5.2 访问控制模型的实现方法 …… 31
2.5.3 安全计算机系统的若干标准 …… 33
2.5.4 安全操作系统的具体实现 …… 35
2.5.5 Windows NT/2K 安全访问控制手段 …… 36
2.5.6 访问控制技术现状与发展 …… 38
第 3 章 访问控制类产品的概况 …… 39
3.1 访问控制类产品概述 …… 39
3.1.1 安全产品的发展趋势 …… 39
3.1.2 访问控制类产品的优势 …… 42
3.2 访问控制类产品介绍 …… 42
3.2.1 安星个人主机防护系统 …… 43
3.2.2 网盾安全专家 …… 44
3.2.3 数码小卫士 …… 48
3.2.4 文件防弹衣 …… 49
第 4 章 访问控制类产品的应用 …… 52
4.1 数码小卫士 …… 52
4.1.1 数码小卫士的安装 …… 52
4.1.2 数码小卫士的使用 …… 55
4.2 其他共享软件 …… 60
4.2.1 加密金刚锁 …… 61
4.2.2 虚拟保险箱 …… 68
4.2.3 冰盾系统安全专家 …… 77
第 5 章 文件防弹衣 …… 87
5.1 文件防弹衣研发概况 …… 87

5.1.1 研发背景 87
5.1.2 实现原理 89
5.1.3 主要特点 91
5.2 文件防弹衣基本功能 92
5.2.1 安装和注册 92
5.2.2 基本准备 94
5.2.3 单一文件或目录保护 96
5.2.4 批量保护设置 98
5.2.5 对受保护文件资源的操作 99
5.2.6 受保护资源的查询与修改 103
5.2.7 解除保护设置 104
5.2.8 一次口令验证的应用 105
5.2.9 脱机保护管理的应用 105
5.3 文件防弹衣管理员功能 106
5.3.1 管理员模式 106
5.3.2 解除保护 107
5.3.3 类型保护 108
5.3.4 高级应用 109
5.3.5 安全策略 110
5.3.6 系统维护 111
5.4 文件防弹衣与其他产品的对比 112
5.4.1 与访问控制类产品的对比 112
5.4.2 与其他安全产品的对比 113
第 6 章 网络文件防弹衣 117
6.1 网络文件防弹衣介绍 117
6.1.1 研发背景 117
6.1.2 新亮点 118
6.1.3 创新点 120
6.1.4 关键技术 122
6.2 新增功能 123
6.2.1 加密保护 123
6.2.2 批量加密保护 124
6.2.3 加密文件整理 125

6.2.4 部门信息维护 126
6.2.5 网络发布 127
6.2.6 网络文件管理 128
6.2.7 安全磁盘维护 129
6.2.8 安全策略 132
6.2.9 外设监控 132
6.2.10 日志浏览 134
第 7 章 文件防弹衣防御体系 138
7.1 主动防御体系 138
7.1.1 主动防御体系概述 138
7.1.2 融合技术的发展趋势 139
7.1.3 访问控制技术与其他技术的融合 140
7.2 文件防弹衣的发展方向 141
7.2.1 文件防弹衣防御体系 141
7.2.2 服务器安全问题 143
7.2.3 文件防弹衣服务器版 145
7.2.4 数据库安全问题 147
7.2.5 文件防弹衣数据库版 148
7.2.6 安全中间件概述 153
7.2.7 文件防弹衣中间件版 154
参考文献 157

第 1 章　计算机安全技术

计算机的安全是一个越来越引起世界各国关注的重要问题，也是一个十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络被不断非法入侵，重要资料被窃密，甚至由此造成网络系统的瘫痪等，已给各个国家以及众多公司造成巨大的经济损失，甚至还危害到国家和地区的安全。因此计算机系统的安全问题是一个关系到人类生活与生存的大事情，必须给予充分的重视并设法解决。

1.1　计算机安全技术概况

在网络出现以前，计算机信息安全指对信息的机密性、完整性和可获性的保护，即面向数据的安全。互联网出现以后，信息安全除了上述内容外，其外延又扩展到面向用户的安全，即鉴别、授权、访问控制、抗否认性和可服务性，以及在内容方面的个人隐私、知识产权等的保护。这两者的结合就是现代的信息安全体系结构。

1.1.1　计算机安全概述

计算机安全从其本质上讲就是计算机系统上信息的安全，指网络系统的硬件、软件及其系统中的数据的安全。计算机信息的传输、存储、处理和使用都要求处于安全的状态。

计算机安全事故发生的几个主要原因如下：

（1）现有计算机系统和网络协议还是不健全、不完善、不安全的。

（2）思想麻痹，没有清醒地意识到黑客入侵所导致的严重后果，舍不得投入必要的人力、财力和物力来加强网络的安全性。

（3）没有采取正确的安全策略和安全机制。

（4）缺乏先进的计算机安全技术、工具、手段和产品。

（5）缺乏先进的灾难恢复措施和备份意识。

计算机安全根据其本质的界定，应具有以下的基本特征。

（1）保密性：保密性是指信息不泄露给非授权的个人、实体，或供其使用的特性。

（2）完整性：完整性是指信息未经授权不被修改、不被破坏、不被插入、不延迟、不

乱序和不丢失的特性。对网络信息安全进行攻击的最终目的就是破坏信息的完整性。

（3）可用性：可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。

（4）可控性：可控性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及方式。

（5）可审查性：在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

1.1.2 计算机信息安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。该安全策略不但要靠先进的技术，而且也得靠严格的管理、法律约束和安全教育，主要包括以下内容。

（1）威严的法律：安全的基石是社会法律、法规和手段，即通过建立与信息安全相关的法律法规，使非法分子慑于法律，不敢轻举妄动。

（2）先进的技术：先进的技术是信息安全的根本保障，用户对面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。

（3）严格的管理：各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

计算机安全策略是一个系统的概念，它是计算机安全系统的灵魂与核心，任何可靠的计算机安全系统都是架构在各种安全技术的集成的基础上的，而计算机安全策略的提出，是为了实现这种技术的集成。计算机安全策略是为了保护计算机安全而制定的法律、法规和措施的总和。当前制定的计算机安全策略主要包含下述 5 个方面的策略。

（1）物理安全策略。物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件设备和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种盗窃、破坏活动的发生。

（2）访问控制策略。访问控制是计算机安全防范和包含的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它也是维护网络系统安全，保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到安全作用，但访问控制是保证计算机安全最重要的核心策略之一。它主要由入网访问控制、网络权限控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络检测和锁定控制及网络端口和节点的安全控制组成。

（3）防火墙控制策略。它是控制进出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

（4）信息加密策略。信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。常用的方法有链路加密、端到端加密和节点加密。链路加密的目的是保护网络节点之间的链路信息安全，端到端加密的目的是对源端用户到目的端用户的数据提供保护，节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

（5）计算机安全管理策略。在计算机安全中，除了采用上述措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络的安全和可靠的运行，将起到十分有效的作用。网络的安全管理策略包括确定安全管理的等级和安全管理的范围，制定有关网络使用规程和人员出入机房管理制度，制定网络系统的维护制度和应急措施等。随着网络技术的发展，计算机网络将日益成为工业、农业和国防等方面的重要信息交换手段，渗透到社会生活的各个领域。因此认清网络的脆弱性和潜在威胁，采取强有力的安全策略，对于保障网络的安全性将变得十分重要。

1.1.3 计算机安全体系结构与模型

1982年，在开放系统互连（OSI）参考模型建立之初，就开始进行了对OSI安全体系结构的研究。1989年12月，ISO（国际标准化组织）颁布了计算机信息系统互连标准的第二部分，即ISO7498-2标准，并首次确定了开放系统互连参考模型的安全体系结构。我国将其称为GB/T9387-2标准，并予以执行。OSI安全体系结构包括3部分内容：安全服务、安全机制和安全管理。

1. 安全服务

安全服务是由参与通信的开放系统的某一层所提供的服务，它确保了该系统或数据传输具有足够的安全性。OSI安全体系结构确定了5大类安全服务：认证、访问控制、数据保密性、数据完整性和不可否认（抗抵赖）。下面分别予以介绍。

（1）认证服务。这种安全服务提供某个实体的身份保证。该服务有两种类型：对等实体认证和数据源认证。

（2）访问控制服务。这种安全服务提供的保护，就是对某一些确知身份的限制、对某些资源（这些资源可能是通过OSI协议可访问的OSI资源或非OSI资源）的访问。这种安全服务可用于对某个资源的各类访问（如通信资源的利用，信息资源的阅读、书写或删除，处理资源的执行等）或用于对某些资源的所有访问。访问控制是实现授权的一种方法，它涉及通信和系统的安全问题。它对通信协议有很高的要求。

（3）数据保密性服务。这种安全服务能够提供保护，使得信息不泄露、不暴露给那些未授权就想掌握该信息的实体。

（4）数据完整性服务。这种安全服务保护数据在存储和传输中的完整性。

（5）不可否认（抗抵赖）服务。该服务主要保护通信系统不会遭到自系统中其他合法用户的威胁，而不是来自未知攻击者的威胁。

2. 安全机制

为了支持以上的安全服务，OSI 安全体系结构定义了 8 大类安全机制：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务填充机制、路由控制机制和公证机制。这些安全机制可以设置在适当的层次上，以便提供某些安全服务。

（1）加密机制。加密可向数据或业务流信息提供保密性，并能对其他安全机制起作用或对它们进行补充。加密算法可以是可逆或不可逆的。

（2）数字签名机制。这种安全机制由两个过程构成：对数据单元签名过程和验证签名的数据单元过程。第一个过程可以利用签名者私有的（独有和保密的）信息，而第二个过程则要利用公之于众的规程和信息，但通过它们并不能推断出签名者的私有信息。

（3）访问控制机制。这种安全机制可以利用某个实体经鉴别的身份或关于该实体的信息（如某个已知实体集里的一员），进行确定并实施实体的访问权。如果该实体试图利用未被授权的资源或用不正当的访问方式使用授权的资源，那么访问控制功能将会拒绝这个企图，另外还可能产生一个告警信号或把它作为安全审计线索的一部分记录下来，并以此报告这一事件。对于无连接数据的传输，则只有在数据源强制实施访问控制之后，才有可能向发信者提出任何拒绝访问的通知。

（4）数据完整性机制。数据完整性机制主要包括两个方面：单个的数据单元或字段的完整性、数据单元串或字段串的完整性。

（5）鉴别交换机制。这种安全机制是通过信息交换以确保实体身份的一种机制。

（6）业务填充机制。能用来提供各种不同级别的保护，抵抗通信业务分析。这种机制只有在通信业务填充受到机密服务保护时才是有效的。

（7）路由控制机制。路由控制机制提供了这样一种机制，它可以控制和过滤通过路由器。

（8）公证机制。这种保证是由第三方公证人提供的，公证人为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。

1.2　计算机安全技术分类

计算机信息安全的技术涵盖的范围非常广泛，以下主要对其中的加密技术、防火墙技术、入侵检测技术、病毒防范技术、访问控制技术 5 种关键技术做简单的介绍。

1.2.1　加密技术

1. 基本概念

加密技术（或密码学）是研究通信安全保密的一门学科，它包含两个相对独立的分支：密码编码学和密码分析学。前者是研究把信息（明文）变换成没有密钥就不能解读或很难解读的密文的方法，从事此行的人称为密码编码者；后者是研究分析破译密码的方法，从事此行的人称为密码分析者。密码编码学和密码分析学彼此的目的相反，相互独立，但在发展中又相互促进。密码编码学的任务是寻求生成高强度密码的有效算法，以满足对信息进行加密或认证的要求；密码分析学的任务是破译密码或伪造认证密码，窃取机密信息进行诈骗破坏活动。对一个保密系统采取截获密文进行分析的方法来进行的攻击称为被动攻击；非法入侵者采用删除、更改、添加、重放、伪造等手段向系统注入假信息的攻击称为主动攻击。进攻与反进攻、破译与反破译是密码学中永无止境的矛与盾的竞技。

密码技术普遍依赖于数学。一般而言，越是先进的加密算法，其所涉及的数学也越高深；而随着计算机科技的进步，加密技术日新月异，原来不能破解的加密技术也可能因为计算速度的提高和计算机成本的降低而变得容易。所以，每当出现新的加密技术时，破解技术亦尾随而至，加密与解密一直如同白道与黑道一般，经常是道高一尺，魔高一丈。

2. 加密技术的起源与发展

加密技术（或密码学）是一门既古老又年轻的学科，其历史可以追溯到几千年以前。早在 4000 多年以前，古埃及人就开始使用密码技术对待传递的消息进行加密。此外，古代的一些行帮暗语及文字加密游戏等，实际上也是对信息的加密，这种加密通过一定的约定，把需要表达的信息限定在一定范围内流通。第一次世界大战前，密码技术的进展很少公布于众。直到 1918 年，William F. Friedman 的论文“The Index of Coincidence and Its Applications in Cryptography（重合指数及其在密码学中的应用）”发表后，情况才有所好转。在这漫长的时期内，信息的保密基本上靠人工对消息加密、传输和防破译；其应用也主要局限于军事目的，只为少数人掌握和控制。所以，它的发展受到了限制。这就是古典密码技术阶段，也是密码技术的起源。在这一时期，密码技术基本上可以说是一门技巧性

很强的艺术，而不是一门科学。密码学专家常常也是凭借自己的直觉和信念来进行密码设计和分析，而对密码的分析也大多数是基于密码分析者（即破译者）的直觉和经验。

1949 年，C. E. Shannon（香农）在《贝尔系统技术杂志》上发表了“The Communication Theory of Secrecy System（保密系统的通信理论）”一文，为密码技术奠定了坚实的理论基础，使密码学真正成为一门科学。但是，科学理论的产生并没有使密码学丧失艺术性的一面，直到今天，密码技术仍是一门非常有艺术的学科。直到 1967 年，由于保密的需要，人们基本上看不到有关密码学的文献和资料。1967 年，David Kahn（戴维·卡恩）通过《The Codebreakers（破译者）》一书全面地阐述了密码技术理论，激发了许多研究者和生产商的兴趣，使现代密码技术及其应用得到了飞速的发展。目前，现代密码技术已经深入到信息安全的各个环节和对象，其应用已不仅仅局限于政治、军事等领域，其商用价值和社会价值也得到了充分的肯定。

当前，计算机网络的广泛应用，产生了大量的电子数据，这些数据需要传输到网络的各个地方并存储。这些数据有的具有重大的经济价值，有的关系到国家、军队或企业的命脉，甚至生死存亡。对于这些数据，有意的计算机犯罪或无意的数据破坏都可能造成不可估量的损失。对于这些行为，光靠法律和相应的监督措施很难满足现实的需要，必须进行自我保护。因此，理论和事实都说明密码技术是一种实用而有效的方法。这也是现代密码技术得到快速发展和广泛应用的原因。

3. 密码技术的分类

密码技术的分类有很多种标准，如按执行的操作方式不同，可以分为替换密码技术（Substitution Cryptosystem）和换位密码技术（Permutation Cryptosystem）。从使用的密钥角度而言，密码技术分为对称密码技术和非对称密码技术。对称密码技术中，加密和解密的双方拥有相同的密钥；非对称密码技术中，加密和解密的双方拥有不同的密钥。

在对称密码技术中，其加密密钥和解密密钥相同。加密信息的安全性取决于密钥的安全性，与算法的安全性无关，即由密文和加解密算法不可能得到明文。换句话说，算法无需保密，需保密的仅是密钥。对称密码技术对明文的加密有两种方式：一是明文信息按字符（如二元数字）逐位地加密，称为流密码技术；二是将明文信息分组（含多个字符），逐组进行加密，称为分组密码。非对称密码技术的主要特点是将加密和解密能力分开，加密密钥（即公开密钥）PK 是公开的，加密算法 E 和解密算法 D 也都是公开的，而解密密钥（也称为秘密密钥）SK 是保密的。虽然 SK 是由 PK 决定的，但不能根据 PK 计算出 SK，即加密密钥和解密密钥在计算上是不能相互推算出的。

4. 加密技术的应用

加密技术在计算机系统中得到大量的应用，其中比较典型的应用有下述几种。

（1）PKI（公钥基础设施）技术：这是一种利用公钥密码理论和技术建立起来的提供信息安全服务的基础设施，旨在从技术上解决网上身份认证、信息的完整性和不可抵赖性等安全问题，为电子商务、电子政务、网上银行和网上证券等网络应用提供可靠的安全服务的基础设施。用户利用PKI所提供的安全服务，在网上实现安全通信，透明地提供加/解密和数字签名等密码服务所需要的密钥和证书管理。PKI提供的安全服务对用户来说是完全透明的，它的安全服务形式和电力服务系统的提供服务截然不同，例如，电灯通过亮与不亮就可以感觉电力系统的服务是否存在，而PKI提供的安全服务隐藏在其他应用的后面，用户无法直观地感觉到它是否有效或在起作用。

（2）PMI（授权管理基础设施）技术：这是国家信息安全基础设施NISI（即National Information Security Infrastructure, NISI由PKI和PMI组成，其中，公钥基础设施构成所谓的PKI信息安全平台，提供智能化的信任服务；而授权管理基础设施（PMI）构成所谓的授权管理平台，在PKI信息安全平台的基础上提供智能化的授权服务）的一个重要组成部分，目标是向用户和应用程序提供授权管理服务，提供用户身份到应用授权的映射功能，提供与实际应用处理模式相对应的，与具体应用系统开发、管理无关的授权和访问控制机制，简化具体应用系统的开发与维护。

PMI以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理，即由资源的所有者进行访问控制。与PKI相比，两者的主要区别：PKI证明用户是谁，而PMI证明这个用户有什么权限，能干什么，而且PMI需要PKI为其提供身份认证。PMI与PKI在结构上是非常相似的。信任的基础都是有关权威机构，由有关权威机构决定建立身份认证系统和属性特权机构。

（3）数字签名技术：在一个保密通信系统中，为了防备通信双方的任何一方的欺骗或伪造，用数字签名（Digital Signature）技术可以有效地解决这个问题。公钥（非对称）密码技术非常适合于数字签名。数字签名和传统的手写签名具有同样的功效，类似于亲笔签名或盖章。那么在计算机网络中传送的信息，如何“亲笔签名或盖章”呢？数字签名是密码技术领域中研究的重要问题之一，是日常生活中手写签名的电子对应物，它的主要功能是实现用户以电子信息形式存放信息的认证。当今，随着电子商务技术的迅速发展，数字签名的使用将会越来越普遍。

1.2.2 防火墙技术

所谓防火墙，是指一种将内部网和公众网络（如Internet）分开的方法，它实际上是一

种隔离技术，是在两个网络通信时执行的一种访问控制手段，它允许用户“同意”的人和数据进入网络，同时将用户“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问自己的网络，防止他们更改、复制和毁坏自己的重要信息。

1．防火墙的目标

（1）对于一个网络来说，所有通过“内部”和“外部”的网络信息流量都要经过防火墙。

（2）通过一些安全策略，来保证只有经过授权的信息流量才可以通过防火墙。

（3）防火墙本身必须建立在安全操作系统的基础上。

2．防火墙的优点

（1）防火墙对企业内部网实现了集中的安全管理，可以强化计算机安全策略，比分散的主机管理更经济易行。

（2）防火墙能防止非授权用户进入内部网络。

（3）防火墙可以方便地监视网络的安全性并报警。

（4）可以作为部署网络地址转换（Network Address Translation）的地点，利用网络地址转换技术，可以缓解地址空间的短缺，隐藏内部网的结构。

（5）利用防火墙对内部网络的划分，可以实现重点网段的分离，从而限制问题的扩散。

（6）由于所有的访问都经过防火墙，所以防火墙是审计和记录网络的访问和使用的最佳地方。

3．防火墙的局限性

（1）限制有用的网络服务。防火墙为了提高被保护网络的安全性，限制或关闭了很多有用但存在安全缺陷的网络服务。

（2）无法防护内部网络用户的攻击。目前，防火墙只提供对外部网络用户攻击的防护，对来自内部网络用户的攻击只能依靠内部网络主机系统的安全性。

（3）Internet 防火墙无法防范通过防火墙以外的其他途径的攻击。例如，在一个被保护的网络上只要有一个没有限制的拨出存在，内部网络上的用户就可以直接通过 SLIP（串行线路 IP）或 PPP（点对点协议）连接进入 Internet。

（4）Internet 防火墙也不能完全防止传送已感染病毒的软件或文件。

（5）防火墙无法防范数据驱动型的攻击。数据驱动型的攻击从表面上看是无害的数据被邮寄或复制到 Internet 主机上，但一旦执行就开始攻击。例如，一个数据型攻击可能导