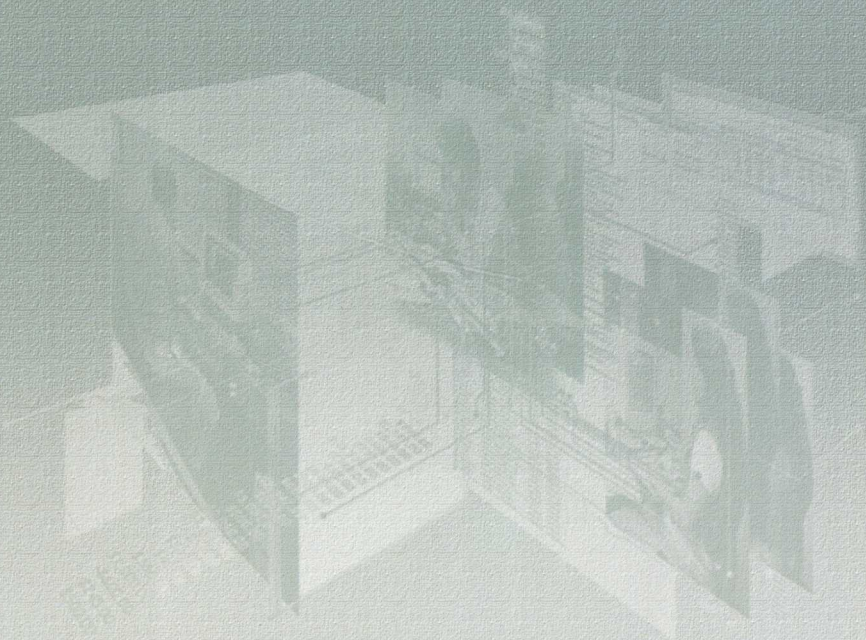
基于角色的访问控制技术

jiyu jiaose de fangwen kongzhi jishu

■ 主 编 刘 强

■ 副主编 陈新度 吴 磊 王 磊 李黎明



华南理工大学出版社

基于角色的访问控制技术

主　编　刘　强
副主编　陈新度　吴　磊　王　磊　李黎明

华南理工大学出版社
·广州·

图书在版编目（CIP）数据

基于角色的访问控制技术 / 刘强主编. —广州：华南理工大学出版社，2010.12
ISBN 978-7-5623-3377-7

Ⅰ. ①基… Ⅱ. ①刘… Ⅲ. ①电子计算机-安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2010）第 249869 号

总 发 行：华南理工大学出版社（广州五山华南理工大学 17 号楼，邮编 510640）
营销部电话：020-87113487 87110964 87111048（传真）
E-mail：scutc13@scut.edu.cn http：//www.scutpress.com.cn
责任编辑：兰新文
印 刷 者：广东省农垦总局印刷厂
开 本：787mm×1092mm 1/16 印张：9 字数：208 千
版 次：2010 年 12 月第 1 版 2010 年 12 月第 1 次印刷
定 价：26.00 元

版权所有 盗版必究

前　言

访问控制是信息系统重要的基础设施。在国际标准化组织 ISO 的网络安全体系设计标准（ISO 7498 - 2）中，访问控制服务与身份认证服务、数据保密服务、数据完整性服务、不可否认服务并列为五大安全服务功能，共同维系网络信息系统的安全特性。

访问控制的本质就是求解问题公式“who + what + how”，即“谁对什么样的资源能执行什么样的操作”。当问题规模较少、访问控制规则简单、访问控制变更事件不频发时，以控制矩阵作为主要数据结构已足够应对访问控制信息存取、变更和管理的需求。然而，随着应用实体规模的扩大，特别是网络化技术的迅猛发展，一些基于网络的、联盟式的应用实体出现，使得访问控制呈现出更为复杂的特征。

（1）访问控制次数显著增加。用户、资源数量的急剧增加使得原来的控制矩阵呈现组合爆炸的趋势，矩阵中任意一元素的赋值即代表着一次访问控制事件，因而访问控制次数也存在组合爆炸的现象。

（2）访问控制模型的管理逻辑变得复杂。访问控制次数的显著增加，导致系统安全管理员无法处理日以万计的访问控制事件，因而出现了管理权限委派的概念，形成层次化的安全管理员团队。管理权限委派制度导致了管理递归现象的出现，同时，为了避免出现权限泄漏和权限滥用，还需要对被委派的安全管理员施行咨询、审计等业务。这些都大幅度增加了访问控制模型管理逻辑的复杂度。

（3）访问控制策略语义复杂、易出现冲突。策略体现为一种规则，表述访问控制过程中施加给被控主体和客体的约束。当被约束对象数量庞大时，策略数量必然庞大；当被约束对象之间关系发生变更时，策略所表述的约束范畴容易发生扩展、重叠、互斥等现象，从而出现访问控制策略之间语义的冲突。由于数量的庞大，访问控制策略语义冲突的检测和消解一直是访问控制领域中的难题。

笔者所在的科研团队从 2001 年便开始接触基于角色的访问控制模型（Role Based Access Control，RBAC），并致力于这一模型的改进和应用。在这一过程中，我们逐步体会到模型中所蕴含的管理思想与委派制式，也逐步认识到模型中的信任、权限泄漏等问题。多年以来，我们针对这些问题开展了深入而系统的研究。

访问控制技术具有重要的理论研究价值和广阔的应用空间。当前，关于这一领域，国内外的研究性论文较多，而进行系统介绍的专著却相对较少。本书编写的目的，就是想抛砖引玉，期望更多的同仁致力于访问控制技术的研究，以实现这一领域技术的发展和突破。

本书的第1、第2章主要介绍访问控制技术的发展和RBAC模型的基本概念；第3章重点阐述RBAC97中的管理思想和安全策略的形式化表述；第4章重点分析RBAC模型中存在的信任，以及由此派生出基于信任的RBAC模型——TB-RBAC；第5、第6章提出了RBAC模型中策略安全分析问题，介绍了基于智能规划的安全分析方法；第7章介绍了笔者所开发的安全分析系统原型；第8章介绍了RBAC模型中的审计方法。本书较深入地分析了访问控制模型中的思想和存在的问题，某些方面仍可以持续深入地研究。因此，本书主要面向科研工作者，也可以作为相关计算机工作者、工程技术人员、研究生的参考书籍。

本书由广东工业大学机电学院计算机集成制造实验室组织编写，刘强副教授负责全书的行文组织和结构设计，陈新度教授对全书进行了审校，吴磊博士与广东科贸职业学院的王磊设计了全书的案例，海军兵种指挥学院李黎明副教授编写了第8章的内容。

在此，还要向诸多老师、朋友表示深深的感谢，感谢中山大学姜云飞教授给予的理论指导，感谢广东工业大学饶东宁博士提出的宝贵建议，感谢成都理工大学刘金花同学为本书进行了文字校对。特别感谢华南理工大学出版社所给予的支持。

由于作者水平有限，本书又涉及一些相对前沿的内容，难免出现纰漏和错误，诚望读者不吝指教。

广东工业大学
刘强
2010年11月

资助项目：国家科技支撑计划项目（2006BAF01A41）
广东省自然科学基金项目（05200197）
广东省科技计划项目（2010B010600035）

目　录

第 1 章　概论 …… 1

1.1　信息系统 …… 1
1.2　信息系统安全及相关技术 …… 2
1.3　访问控制模型 …… 3
1.3.1　访问控制的基本概念 …… 3
1.3.2　自主访问控制模型 …… 4
1.3.3　强制访问控制模型 …… 6
1.3.4　基于角色的访问控制模型 …… 8
1.4　小结 …… 8

第 2 章　RBAC96 …… 11

2.1　RBAC 概述 …… 11
2.2　RBAC96 概述 …… 12
2.3　RBAC96 的形式化描述 …… 14
2.4　RBAC96 的关键技术与概念 …… 14
2.4.1　角色层次与角色继承 …… 14
2.4.2　约束 …… 16
2.5　RBAC96 系统的设计与案例 …… 17
2.5.1　设计说明 …… 17
2.5.2　设计案例——小型应用系统的访问控制系统设计 …… 20
2.6　小结 …… 28

第 3 章　ARBAC97 …… 29

3.1　ARBAC97 模型 …… 29
3.2　ARBAC97 的辖域 …… 30
3.3　ARBAC97 中的管理学含义 …… 31
3.3.1　管理要素 …… 31
3.3.2　RBAC 管理中的组织形态 …… 32
3.3.3　RBAC 管理中的控制方式 …… 32
3.3.4　管理主体之间委派制式 …… 32

3.4 ARBAC97 中存在的问题 …… 33
3.4.1 角色层次关系变更过程中的附带效应 …… 33
3.4.2 管理递归问题 …… 36
3.5 衍生的访问控制模型 …… 37
3.5.1 ARBAC02 与 SARBAC …… 37
3.5.2 时态 RBAC 模型与基于任务的 RBAC 模型 …… 37
3.6 安全策略设计案例——ASP 系统中访问控制策略 …… 38
3.6.1 ASP 系统访问控制需求分析 …… 38
3.6.2 访问控制策略的设置 …… 41
3.6.3 应用示例 …… 43
3.7 小结 …… 44

第 4 章 TB-ARBAC 模型 …… 46

4.1 信任的基本概念 …… 46
4.2 基于信任的 ARBAC 管理模型——TB-ARBAC …… 47
4.3 TB-ARBAC 的信任 …… 50
4.3.1 TB-ARBAC 模型的信任函数 …… 50
4.3.2 TB-ARBAC 模型的信任制度设计 …… 51
4.4 TB-ARBAC 与 ARBAC97 管理模式的对比 …… 52
4.5 小结 …… 53

第 5 章 TB-ARBAC 的安全分析问题 …… 55

5.1 安全策略的形式化 …… 55
5.2 安全状态转移系统 …… 56
5.3 安全策略的安全分析 …… 58
5.4 小结 …… 60

第 6 章 安全分析方法 …… 62

6.1 智能规划技术 …… 62
6.1.1 智能规划的研究历程 …… 62
6.1.2 图规划技术 …… 63
6.1.3 智能规划领域与问题的表示 …… 66
6.2 安全分析过程中的智能规划问题 …… 68
6.3 安全分析的建模过程 …… 69
6.3.1 领域描述和前提假设 …… 69
6.3.2 前置处理 …… 70

6.3.3　领域模型建模的基本步骤 …… 71
6.3.4　从角色继承层次关系到虚动作 …… 73
6.3.5　领域命题互斥的生成 …… 73
6.3.6　从管理策略到规划动作模型 …… 74
6.3.7　规划问题的定义 …… 74
6.3.8　规划解到安全分析领域的翻译 …… 75
6.4　建模过程的复杂性分析 …… 75
6.5　面向安全分析的图规划算法改造策略 …… 75
6.5.1　关于动作与命题互斥的推论 …… 75
6.6　规划图的剪枝 …… 76
6.6.1　领域约束的生成 …… 79
6.6.2　虚动作的剪枝 …… 80
6.6.3　目标状态的生成 …… 81
6.7　Graphplan 算法的改造 …… 82
6.8　小结 …… 84

第 7 章　安全分析原型系统 PolicyProber …… 86

7.1　PolicyProber 简介 …… 86
7.2　系统功能框架和技术框架 …… 86
7.3　PolicyProber 的技术要点 …… 87
7.3.1　规划图的数据结构定义 …… 87
7.3.2　改造后的 GraphPlan 算法的编码 …… 88
7.3.3　PolicyProber 中规划图的显示方式 …… 91
7.4　PolicyProber 操作界面 …… 92
7.5　应用案例说明 …… 92
7.5.1　构造领域模型 …… 93
7.5.2　构造安全分析实例的规划问题 …… 99
7.5.3　求解规划问题 …… 99
7.5.4　基于信任协商的解决方案 …… 99
7.6　小结 …… 101

第 8 章　TB-RBAC 模型中的审计 …… 103

8.1　引言 …… 103
8.2　信息安全审计 …… 103
8.3　TB-ARBAC 中的审计 …… 104
8.4　TB-ARBAC 模型中审计信息的访问控制 …… 106

8.4.1 审计信息组成 …… 106
8.4.2 审计信息的用途分析和存储管理 …… 106
8.4.3 审计信息的访问控制 …… 107
8.5 TB-ARBAC 中的委派制式和权责制度 …… 107
8.6 审计方法 …… 108
8.6.1 常规审计方法 …… 108
8.6.2 事故审计方法 …… 109
8.7 小结 …… 111
附录 安全分析方法的核心代码 …… 112

第1章 概 论

21世纪是信息的时代，信息化已成为时代的手笔，刻画着各行各业改革和发展的方向，信息系统作为信息化的有形实体和重要基础设施越来越彰显其重要性。信息系统安全提供确保信息要素安全和信息系统结构安全的相关技术、服务和管理，是信息系统正常、有效、安全运行的保障。

1.1 信息系统

信息系统（Information System）是一种对各种输入的数据进行加工、处理，产生针对解决某些方面问题的数据和信息。其主要内容是为产生决策信息而按照一定要求设计的一套有组织的应用程序系统。直观地说，信息系统是以提供信息服务为主要目的的数据密集型、人机交互的计算机应用系统。数据作为信息的载体，贯穿于信息系统的始终，在信息系统中存在大量的分类数据，包括原始数据、加工数据、功能型数据、缓存数据等。信息系统具有其基本结构，分为4个层次。

（1）硬件、操作系统和网络层，是信息系统开发和运行的支撑环境；

（2）数据管理层，信息系统的基础设施，包括数据的采集、传输、存取和管理，一般以数据库管理系统（DBMS）作为其核心软件；

（3）应用层，与具体应用环境密切相关，直接反映信息系统的职能，包括各种应用程序，例如分析、统计、报表、规划、决策等；

（4）用户接口层，是信息系统的用户进行系统操作、与系统进行交互的界面层。

信息系统是一种应用广泛的计算机应用系统，管理信息系统、地理信息系统、指挥信息系统、决策支持系统、办公信息系统、科学信息系统、情报检索系统、医学信息系统、银行信息系统、民航订票系统等都属于这个范畴。从技术上而言，信息系统具有如下特点。

（1）存在大容量数据的持久性存储方案。一般而言，原始数据、加工数据、功能型数据需存放在辅助的存储器中，长期保留在计算机系统中。

（2）数据的缓存机制。缓存数据用于瞬态显示和中间计算，在信息系统的运行过程中段时间存在，信息系统在软件和硬件配置上支撑这一缓存机制。

（3）复杂的数据处理加工功能和信息服务职能。信息系统除具有数据采集、传输、存储和管理等基本功能外，还可向用户提供信息检索、统计报表、事务处理、规划、设计、指挥、控制、决策、报警、提示、咨询等信息服务。

（4）信息系统的可复制性。信息系统是可以被复制的，无论是功能、性能，还是运行环境都可以复现，并可以通过修正、调整、配置等手段，适用于另外的相似应用环境。

1.2 信息系统安全及相关技术

信息安全指的是信息的保密性、完整性和可用性。

- 保密性是指保护信息不被非授权的泄露；
- 完整性是指保护信息不遭非授权的破坏；
- 可用性则是指对授权者提供信息的方便、有效使用。

信息安全并不仅仅是指对信息的保护，而应该是对信息系统的安全运行和对运行在信息系统中的信息进行保护（包括信息的保密性、完整性和可用性保护）的总称。信息系统安全就是在信息系统的正常运行过程中，信息的机密性、完整性、可复用性、抗抵赖性、可审计性等特性得以保持。信息系统的安全运行是信息系统提供有效服务（即可用性）的前提。

信息系统具有明确的安全目标：集中体现为信息保护和系统保护。信息保护指保护机要信息在信息系统正常运行过程中的机密性、完整性、可复用性和抗抵赖性等特性；系统保护指保护信息系统正常运行所需要的可靠、稳定、完整等特性。具体的信息系统安全目标依赖于其所服务的组织的安全诉求，与组织的安全利益目标是一致的。

在信息技术高速发展过程中，逐步发展了保持信息系统安全的一系列技术手段。

（1）信息加密。信息加密用来保证信息的机密性。其原理就是将有用的信息转化为看似无用的乱码，使攻击者无法读懂信息的内容从而保护信息。信息加密是保障信息安全的最基本、最核心的技术措施和理论基础。

（2）数字签名。数字签名是在数据单元上附加数据，或对数据单元进行密码变换，通过这一附加数据或密码变换，使数据单元的接收者可以证实数据单元的来源和完整性，同时对数据进行保护。数字签名可以用来保持信息的完整性和抗抵赖性。数字签名机制取决于两个过程：① 签名过程。利用签名者的私有信息作为密钥，或对数据单元进行加密，或产生数据单元的密码校验值。② 验证过程。利用公开的规程和信息来确定签名是否是利用该签名者的私有信息产生的。

（3）身份鉴别。身份鉴别是信息安全的基本机制。用户进入信息系统前，需要提供认证信息给信息系统进行身份鉴别，以保证合法的用户可以进入系统获取相应的操作权限，同时拒绝非法用户的进入。通常有三类验证方法：一是基于口令的身份鉴别，用户被要求提供口令、密钥等；二是基于令牌的身份鉴别，用户被要求提供智能卡和令牌卡等令牌载体；三是基于用户个体特征的身份鉴别，用户被要求提供指纹、声音、视网膜或签字等信息。

（4）访问控制。访问控制的目的是防止对信息资源的非授权访问和非授权操作，

用以保持数据的完整性和机密性。访问控制采用最小特权原则，即在给用户分配权限时，根据每个用户的任务特点使其获得完成自身任务的最低权限，不给用户赋予其工作范围之外的任何权力。

（5）安全审计。安全审计是防止内部犯罪和事故后调查取证的基础，通过对一些重要事件的记录，从而在系统发现错误或受到攻击时能定位错误和找到攻击成功的原因。安全审计是一种很有价值的安全机制，可以通过事后的安全审计来检测和调查安全策略执行的情况以及安全遭到破坏的情况。安全审计需要记录与安全有关的信息，通过明确所记录的与安全有关的时间的类别，安全审计跟踪信息的收集可以适应各种安全需要。审计技术能使信息系统自动记录机器的使用时间、敏感操作和违纪操作等。安全审计跟踪对潜在的安全攻击源的攻击起到威慑作用。

（6）网络控制技术。网络控制技术主要针对以迅速发展的分布式和网络化信息系统而言，包括防火墙技术、入侵检测技术等。

①防火墙技术。防火墙是一种既可允许接入外部网络，同时又能够识别和抵抗非授权访问的安全技术。

②入侵检测技术。入侵检测技术扫描当前网络的活动，监视和记录网络的流量，根据已定义的规则过滤主机网卡到网线上的流量，提供实时报警。

1.3　访问控制模型

访问控制模型是实现信息系统安全的重要基础设施。在国际标准化组织 ISO（International Organization for Standardization）的网络安全体系设计标准（ISO 7498—2）中，访问控制服务与身份认证服务、数据保密服务、数据完整性服务、不可否认服务并列为五大安全服务功能，共同维持网络系统的安全特性[1]。访问控制通过适当的访问权限管理来实现系统的信息和资源保护，防止用户对系统信息进行非法访问。

1.3.1　访问控制的基本概念

访问控制模型及相关技术的研究可追溯到 20 世纪 60 年代末，它的基本目标是防止非法用户进入系统和对系统资源的非法使用。为了达到这个目标，访问控制常以主体身份的准确认证为前提，定义并实施各种访问控制策略，来控制和规范合法主体在系统中的对客体的行为。因此，访问控制包括三大要素：主体、客体和控制策略。

（1）主体（Subject）。主体是对其他实体施加动作的主动实体，简记为 S。有时，作为主体的用户（User）或其他访问者（被授权使用计算机的人员），也被记为 U。主体的含义是广泛的，可以是用户所在的组织、用户本身，也可是用户使用的计算机终端、卡机、手持终端（无线）、应用服务程序或进程。

（2）客体（Object）。客体是接受其他实体访问的被动实体，简记为 O。客体的概念也很广泛，凡是可以被操作的信息、资源、对象都可以认为是客体。在信息社会中，

客体可以是信息、文件、记录等的集合体，也可以是网路上的硬件设施、无线通信中的终端，甚至一个客体可以包含另外一个客体。

（3）控制策略（Policy）。控制策略指规范主体对客体的操作行为规则集和约束条件集。简单讲，控制策略是主体对客体的访问规则集，这个规则集直接定义了主体可以对客体实施的行为或禁止主体对客体实施的行为，以及实施过程中所需满足的条件约束。访问策略分为定义和执行两块的内容，系统实施之初，系统安全管理员依据定义控制策略进行授权，在系统运行过程中，依据授权规则，主体的操作行为被规范化和约束执行。

访问控制的实现首先要考虑对合法用户进行验证，然后是对控制策略的选用与管理，最后要对非法用户或是越权操作进行管理。所以，访问控制包括认证、控制策略实现和审计三方面的内容。

（1）认证。主体对客体的识别认证和客体对主体检验认证。主体和客体的认证关系是相互的，当一个主体受到另外一个客体的访问时，这个主体也就变成了客体。一个实体可以在某一时刻是主体，而在另一时刻是客体，这取决于当前实体的功能是动作的执行者还是动作的被执行者。

（2）控制策略实现。如何设定规则集合从而确保正常用户对信息资源的合法使用，既要防止非法用户，也要考虑敏感资源的泄漏，对于合法用户而言，更不能越权行使控制策略所赋予其权利以外的功能。

（3）审计。审计的重要意义在于，比如客体的管理者即管理员有操作赋予权，他有可能滥用这一权利，这是无法在策略中加以约束的。必须对这些行为进行记录，从而达到威慑和保证访问控制正常实现的目的。

在访问控制的研究历程中，先后出现了一系列的访问控制模型。

1.3.2 自主访问控制模型

1971 年，Lampson 等学者提出了著名的访问控制矩阵模型（Access Control Matrix）[2]，主体（Subject）、客体（Object）、访问权限（Permission）等一系列概念被定义并为后世沿用。主体、客体之间的访问关系构成二维矩阵，元素的取值就是相应主体对客体的访问权限，如读（read）、写（write）等。访问控制矩阵模型中，客体的所有者（Owner）完全拥有被控对象的权限，并依据授权规则进行授权。基于 Lampson 的访问控制矩阵模型，Graham 和 Denning 对自主访问控制授权规则进行了研究[3]。1976 年，M. A. Harrison，W. L. Ruzzo，J. D. Ullman 对 Lampson 模型进行了拓展，提出形式化模型 HRU（Harrison-Ruzzo-Ullman Model）[4]，其后，以 Lampson 模型为基础相继出现了系列模型[5,6,7,8,9,10,11]，构成了自主访问控制（Discretionary Access Control，DAC）的主要研究线路。

自主访问的含义是拥有访问许可的主体能够直接或间接地向其他主体转让访问权。自主访问控制模型（Discretionary Access Control，DAC）是根据自主访问控制策略建立

的一种模型，自主访问控制模型在确认主体身份以及（或）它们所属的组的基础上，控制主体的活动，实施权限管理、访问属性（读、写、执行）管理等。

基于访问控制矩阵的访问控制表（Access Control List，ACL）是自主访问控制中通常采用的一种安全机制。ACL 是带有访问权限的矩阵，这些访问权限是授予主体访问某一客体的。安全管理员通过维护 ACL 来控制主体访问客体。对每一个受保护的资源，ACL 对应一个个人用户列表或由个人用户构成的组列表，表中规定了相应的访问模式或操作权限。

基于 ACL 的自主访问控制是细粒度，单用户、单资源级别的。当信息系统的用户庞大、资源数众多时，权限管理数据量呈现组合爆炸的趋势，ACL 规模异常庞大，主体、客体集二者之间的映射关系发生变化时（如组织内的人员、工作职能发生变化），访问控制列表的维护、更新工作异常困难。一般而言，基于访问控制列表机制管理授权只能面向小规模、轻量化的应用对象。其复杂的管理模式易于出错，且这种策略也存在不能保证信息传输的安全性等隐患，因为入侵者有很多方法绕过验证来获得资源。

自主访问控制的主要特征体现在主体可以自主地把自己所拥有的客体访问权限授予其他主体或者从其他主体收回所授予的权限。没有存取权的主体只允许由授权主体指定对客体的访问权。自主访问控制的缺点是信息在移动过程中其访问权限关系会被改变，如主体 $s_1 \in S$ 可将其对客体 $o \in O$ 的访问权限传递给主体 $s_2 \in S$，从而使不具备对 o 有访问权限的 s_2 可访问 o。

为了实现完备的自主访问控制系统，由访问控制矩阵提供的信息必须以某种形式存放在系统中。访问矩阵中的每一行表示一个主体，每一列则表示一个受保护的客体，矩阵中的元素表示主体可以对客体的访问模式。逻辑上，访问控制矩阵中，存储着任意一个主体对任意一个客体的访问模式，然而，主体往往只对极小部分的客体拥有访问权限，因此矩阵中大多数的元素为空。大量空元素的存在将会造成存储空间的浪费，查询效率严重下降。实际上，我们常常是用基于矩阵的行或列来表达访问控制信息。

1．基于行的自主访问控制

这种方式是在每个主体上都附加一个该主体可访问的客体的明细表，也称为访问能力表。能力是一个提供给主体对客体具有特定权限的不可伪造的标志。只有当一个主体对某个客体拥有准许访问的能力时，它才能访问这个客体。按照表内存储信息的不同，可以分为以下三种形式。

（1）权利表。该表可确定用户是否可以对客体进行访问，以及可以进行何种访问。

（2）前缀表。包括受保护的客体名和主体对它的访问权。

（3）口令。口令机制是按行表示访问控制矩阵的。每个客体都相应的有一个口令。主体在对客体进行访问前，必须向操作系统提供该客体的口令。

2．基于列的自主访问控制

基于列的访问控制方法是在每个客体上都附加一份可访问它的主体的明细表，也称做访问控制表。访问控制表中的每一项包括主体的身份以及对该客体的访问权。访问控

制表是目前采用最多的一种实现方式。访问控制表可以对某个特定资源指定任意一个用户的访问权限，还可以将有相同权限的主体分组，并授权改组相同的访问权限。还可以用通配符“*”来代替任何组名或主体标识符。

自主访问控制技术一个最主要的缺点，就是不能有效地抵抗计算机病毒的攻击。在自主访问控制技术中，某一合法用户可任意运行一段程序来修改该用户拥有的文件访问控制信息，而操作系统无法区别这种修改是用户自己的合法操作还是计算机病毒的非法操作。因而被用户执行的程序拥有与该用户相同的权限，这意味着系统安全依靠运行的程序。显然，当一个程序中发生安全裂缝时，一定会影响到该用户所能访问的所有对象。这使得 DAC 在特洛伊木马前特别脆弱。例如，假设 Alice 对文件 file1. doc 拥有读写权限。Charlie，一个恶意攻击者，写了一个程序，这个程序在执行时生成文件 file2. doc。这个程序授予 Alice 写权限和 Charlie 读权限。Charlie 把这个程序伪装成合法的程序发给 Alice。当 Alice 运行这个程序时，它就具有和 Alice 相同的权限，它可以拷贝 file1. doc 到 file2. doc，这样 Charlie 就窃取了 file1. doc 的内容。显然，如果一个安全管理员执行这样的木马程序，攻击者会获取最大的特权，危害整个系统的安全，这成了自主访问控制技术的软肋。此外，自主访问控制技术也没有什么一般的方法能够防止计算机病毒将信息通过共享客体从一个进程传送给另一个进程。为此，必须采用更强有力的访问控制模型。

自主访问控制模型实现简单，在早期得到了广泛的应用。但是由于其允许访问权限的传递，使得传递出去的访问权难以管理和跟踪。此外，DAC 模型无法保护受控资源的副本。当 DAC 模型用于管理主客体数量巨大的系统时，将造成开销巨大、效率低下等问题，因此，其难以满足大型应用，特别是网络应用的需要，仅仅局限于小规模和轻量化的应用对象。

1.3.3 强制访问控制模型

强制访问控制（Mandatory Access Control，MAC）模型最初源于对信息机密性的要求以及防止特洛伊木马之类的攻击，其基本思想是：通过对主体和客体分配固定的安全属性，利用安全属性来决定主体是否可以对客体进行访问。1973 年，D. ElliottBen 和 Leonard. J. L 建立了模拟军事安全策略的访问控制模型——Ben-LaPadula 模型[16]，该模型采用多级安全策略，根据主体和客体在系统中的不同安全级别来控制主体对客体的访问控制。Bida 以 Bell-Lapadula 模型为基础提出 Bida 模型，该模型与 Bell-Lapadula 模型相似，但是强调完整性而不是保密性；Sandhu 在 1993 年提出了基于点阵的访问控制模型[21]，均属于强制访问控制模型的研究范畴。

强制访问控制的含义是指系统强制主体服从访问控制政策。MAC 模型的主要特征是对所有主体及其所控制的客体（例如：进程、文件、段、设备）实施强制访问控制。在 DAC 访问控制中，用户和客体资源都被赋予一定的安全级别，用户不能改变自身和客体的安全级别，只有管理员才能够确定用户和组的访问权限。与 DAC 模型不同的是，

MAC 使用一种多级访问控制策略，系统对访问主体和受控对象实行强制访问控制，其控制方式为：系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。MAC 对访问主体和受控对象标识两个安全标记：一个是具有偏序关系的安全类别标记，包括：绝密级别（Top Secret）、秘密级别（Secret）、机密级别（Confidential）、限制级别（Restricted）和无级别级（Unclassified），其级别为 TS > S > C > R > U。主体和客体可以属于不同的安全等级，安全等级构成一个偏序关系。比如，主体 $s \in S$ 的安全等级为 TS，而客体 $o \in O$ 的安全等级为 S 时，用偏序关系可以表述为SC（s）≥SC（o）（SC 表示安全等级）。另一个是非等级分类标记，不对主体和客体按照安全等级分类，只给出客体接受访问时可以使用的规则和管理者。

通常，系统根据主体和客体的安全敏感性标记来决定其访问模式。考虑到偏序关系，主体对客体的访问模式主要有四种方式。

（1）向下读（Read Down，RD）：主体安全级别高于客体的安全级别时允许读操作；

（2）向上读（Read Up，RU）：主体安全级别低于客体的安全级别时允许的读操作；

（3）向下写（Write Down，WD）：主体安全级别高于客体的安全级别时允许写操作或其他操作；

（4）向上写（Write Up，WU）：主体安全级别低于客体的安全级别时允许写操作或其他操作。

比较知名的 MAC 模型有：Bell-LaPadula 模型和 Biba 模型。Bell-LaPadula 模型具有只允许向下读、向上写的特点，可以有效地防止机密信息向下级泄露；Biba 模型则具有不允许向下读、向上写的特点，可以有效地保护数据的完整性。下面将简要介绍几种主要 MAC 模型：Bell-LaPadula 模型（BLP Model）、Biba 模型（Biba Model）和 Lattice 模型。

1. Bell-LaPadula 模型[12]

Bell-LaPadula 模型（BLP 模型）是典型的信息保密性多级安全模型，其基本的访问控制原则是：①不允许向上读；②不允许向下写。依据此原则，BLP 模型可以有效防止低级用户和进程访问安全级别比它高的信息资源，同时，也阻止安全级别高的用户和进程向比它安全级别低的用户和进程写入数据。BLP 模型的安全策略包括强制访问控制和自主访问控制两部分。强制访问控制体现在：对于给定安全级别的主体，只能对同一安全级别和较低安全级别上的客体进行“读”；只能对相同安全级别或较高安全级别上的客体进行“写”。自主访问控制体现在：允许用户自行定义是否让个人或组织存取数据。

BLP 模型通常是处理多级安全信息系统的设计基础。例如：在处理绝密级数据和秘密级数据时，要防止处理绝密级数据的程序把信息泄露给处理秘密级数据的程序。BLP 模型的出发点是维护系统的保密性，有效地防止信息泄露。然而，BLP 模型只解决了信

息的保密问题，其在完整性定义方面存在一定缺陷。BLP 模型没有采取有效的措施来制约对信息的非授权修改，因此使得非法、越权篡改成为可能。

2. Biba 模型[13,14,15,16]

针对 BLP 模型对数据完整性保护较弱的弱点，Biba 模型基于两种规则来保障数据的完整性和保密性。

（1）下读属性，主体不能读取安全级别低于它的数据。

（2）上写属性，主体不能写入安全级别高于它的数据。

Biba 模型是和 BLP 模型相对立的模型，Biba 模型改正了被 BLP 模型所忽略的信息完整性问题，但在一定程度上却忽视了保密性。例如，一个安全级别为“机密”的用户要访问级别为“秘密”的文档，它将被允许写入该文档，而不能读取。如果它试图访问“高密”级的文档，那么，读取操作将被允许，而写入操作将被拒绝。这样，就使资源的完整性得到了保障，但保密性降低了。

3. Lattice 模型[17]

在 Lattice 模型中，每个资源和用户都服从于一个安全类别（TS，S，C，R，U）。在整个安全模型中，资源对应一个安全类别，用户所对应的安全级别必须比可以使用的客体资源高才能进行访问。Lattice 模型是实现安全分级的系统，这种方案非常适用于需要对信息资源进行明显分类的系统。

1.3.4 基于角色的访问控制模型

MAC 访问控制模型和 DAC 访问控制模型属于传统的访问控制模型。MAC 和 DAC 都有其局限性，当组织规模不断扩大、结构变换频繁时，就出现了大量繁琐的授权变动，权限管理的复杂度呈现指数增长的态势，系统安全管理员的工作将变得非常繁重，使得系统存在安全隐患和安全漏洞。因此，新的访问控制模型和新的授权管理方式应运而生。

基于角色的访问控制模型（Role-Based Access Control，RBAC）[18]诞生于 1992 年。其基本思想是：对系统操作的各种权限不是直接授予具体的用户，而是在用户集合与权限集合之间建立一个角色集合。每一种角色对应一组相应的权限。一旦用户被分配了适当的角色后，该用户就拥有此角色的所有操作权限。这样做的好处是，不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且角色的权限变更比用户的权限变更要少得多，这样将简化用户的权限管理，减少系统的开销。

然而，角色的引入，使得安全策略的逻辑含义变得复杂，同时也可能引发一系列的管理问题，这些将在后续章节中予以详细介绍和分析。

1.4 小结

本章首先综述了信息系统及其相关的安全技术，然后介绍了访问控制技术的发展历程。