Broadview
www.broadview.com.cn

CSAI 希赛.cn

The Way To System Analyst

系统分析师之路

希赛IT教育研发中心 组编
张友生 主编

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

CSAI.cn 希赛®

系统分析师之路

希赛IT教育研发中心 组编
张友生 主编

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

内 容 简 介

本书由希赛IT教育研发中心组织编写，系《中国系统分析员》杂志的精华版本。内容包括技术讲座、系统分析与建模、项目管理、软件测试、过程改进、解决方案、信息化应用、教育认证和顾问之声共10个方面的知识，全部由活跃在软件领域中的高级工程师编写，是作者的实践经验总结，全面反映了系统分析师（系统分析员）的工作范围。

读者通过阅读本书，可以更好地了解系统分析师的工作，掌握系统分析、项目管理及架构设计等方面的技术和管理知识。

本书可作为系统分析师、信息系统项目管理师及系统架构设计师考试的参考书籍和软件工程师进一步深造并发展的学习用书，也可作为系统分析师日常工作的参考手册和计算机专业教师的教学和工作参考书。

图书在版编目（CIP）数据

系统分析师之路 / 张友生主编. —北京：电子工业出版社，2006.6
ISBN 7-121-02496-9

Ⅰ. 系… Ⅱ. 张… Ⅲ. 软件工程－系统分析－工程技术人员－资格考核－自学参考资料 Ⅳ. TP311.5

中国版本图书馆CIP数据核字（2006）第036013号

责任编辑：毕 宁 bn@phei.com.cn
印 刷：北京东光印刷厂
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：787×1092 1/16 印张：24 字数：619千字
印 次：2006年6月第1次印刷
印 数：4000册 定价：48.00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。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。

编写委员会

组　编　希赛 IT 教育研发中心

主　编　张友生

编　委　（按姓名拼音排序）

曹垣亮　曹　伟　陈　庆　陈徐梅　崔启亮

葛　梅　谷剑芳　贺忻炘　黄以宽　李　雄

刘保青　刘明晶　刘云楚　刘　兴　卢琳生

江玲英　马映冰　彭国荣　漆　英　任甲林

田　晖　田俊国　王胜祥　王树文　吴吉义

谢　顺　邢绍志　熊绳祖　徐　锋　徐荣胜

颜建强　杨　飞　杨晋辉　殷建民　张　华

张　骏　朱　勤

前　言

中国系统分析员顾问团（CSAI，希赛）组建于2001年12月28日，是由通过国家考试的系统分析员／系统分析师、信息系统项目管理师、系统架构设计师，以及从事系统分析、架构设计、项目管理工作多年的人士组成的。CSAI下设10个专业委员会，分别按横向和纵向组织，横向有金融信息化专业委员会、制造业信息化专业委员会、计算机教育专业委员会、电子商务与电子政务专业委员会、电信应用专业委员会；纵向有软件工程专业委员会、项目管理专业委员会、数据库应用专业委员会、架构设计专业委员会、网络应用专业委员会。

CSAI的宗旨是加强全国IT高级人才之间的合作与交流，提高工作水平，积极推进国家信息化建设和软件产业化发展。希赛IT教育研发中心是CSAI计算机教育专业委员会的别名，是一个专门从事IT教育研究、教育产品开发、教育书籍编写的组织。为了培养出更多的IT高级人才，希赛IT教育研发中心组织编写了本书。本书内容来自历年的《中国系统分析员》杂志，作为《中国系统分析员》的精华版本。

《中国系统分析员》创刊于2002年6月，从最初的电子杂志发展成为今天的正式印刷版杂志，历经三载春秋，凝聚了CSAI人的心血。

3年前，CSAI华南区首席顾问马映冰先生感叹道："系统分析员是寂寞的。"经过CSAI所有顾问的努力，今天，希赛网及《中国系统分析员》杂志已经成为一个让系统分析员充分展示自己，让社会了解系统分析员的平台。通过这个平台，让我们的能量被社会认识，让我们的能力被社会认可。从而使得系统分析员不再只是一纸证书，而是一群活跃在中国IT界、恪尽职守的精英！今天，我们可以自豪地说，系统分析员不再寂寞！系统分析员已经成为软件业年青一代发展的方向和努力的目标。

3年前，CSAI资深顾问刘兴先生有感而言："援琴鸣弦发清商，短歌微吟不能长，一个人的声音是很微弱的。"可喜的是，有了《中国系统分析员》这块我们自己的园地，已经把一人之言变成了众人之言、群体之言。政府和社会已经意识到，在软件的产业化和行业的信息化进程中，拥有一支强大的生力军——系统分析员！

当然，正如CSAI华北区首席顾问田俊国先生所言，系统分析员不应该是一群容易满足的人，所以这一点点成绩绝对不应该成为我们骄傲的资本，一个人能否有大的作为，关键在于他有多强的使命感和社会责任感，CSAI也不例外。

当然，通过了系统分析员考试，并不意味着可以飘飘然而不思进取，自以为是。而应以此作为新的起点，不断修炼，获取经验和知识，紧跟时代发展的步伐和技术的进步，才能保证自己不会被社会淘汰，才能确保整个系统分析员群体的高素质，才能维护"中国软件产业的脊梁，各行业信息化的精英"的良好形象和口碑，才能履行时代赋予我们

的光荣职责。

要做一个出色的“敢于承担责任的人”，《中国系统分析员》需要广大系统分析员、项目管理人员和软件工程师的呵护。众人拾柴火焰高。笔者希望每一位顾问、每一位系统分析员都能为《中国系统分析员》杂志出谋划策，贡献高质量的稿件。

我们坚信，只要《中国系统分析员》坚持高标准、高质量原则和指导软件工程实践的正确主题，必将能够影响深远，成为软件领域媒体的旗舰，成为软件企业和软件工程技术人员的必读刊物，成为培养软件工程技术人员并促进国内软件工程技术实践水平的权威刊物。

本书由希赛IT教育研发中心组编，由张友生主编。第1章由朱勤、张友生、李雄、殷建民、王胜祥编写；第2章由徐锋、邢绍志、黄以宽、陈庆、刘云楚、杨飞、卢琳生、任甲林、曹伟、谷剑芳、杨晋辉编写；第3章由吴吉义、田俊国、徐荣胜、张华、任甲林编写；第4章由崔启亮、贺炘、张友生编写；第5章由陈徐梅、葛梅、刘保青、漆英、谷剑芳、王树文、谢顺编写；第6章由曹伟、吴吉义、王树文编写；第7章由王胜祥、颜建强、曹垣亮、彭国荣编写；第8章由熊绳祖、张友生、张骏、刘明晶编写；第9章由刘兴、张华、江玲英、吴吉义编写；第10章由刘云楚、田俊国、马映冰、刘兴、田晖编写。

在本书出版之际，笔者要特别感谢电子工业出版社郭立女士的大力帮助。

编写委员会

2006年3月

目　录

目录

CONTENTS

第1章 技术讲座

1.1 数据库安全技术

数据库技术从20世纪60年代中期开始发展，到现在已经成为了一个活跃的学科领域。以数据库为基础的信息系统正成为经济、政务、国防等领域的信息基础设施，数据库中存储的信息的价值也越来越高，因此数据库系统的安全问题也显得越来越重要。在新的网络环境中，数据库系统需要面对更多的安全威胁，针对数据库系统的攻击方式也层出不穷。

1.1.1 数据库安全概述

数据库系统安全控制是指为数据库系统建立的安全保护措施，以保护数据库系统软件和其中的数据不因偶然或恶意的原因而遭到破坏、更改和泄露。目前，数据库系统安全与网络安全、操作系统安全及协议安全一起构成了信息系统安全的4个最主要的研究领域。

20世纪70年代初，美国军方率先发起对多级安全数据库管理系统（Multilevel Secure Database Management System，简称MLS DBMS）的研究。此后，一系列数据库安全模型被提出。

80年代，美国国防部根据军用计算机系统的安全需要，制定了《可信计算机系统安全评估标准》（Trusted Computer System Evaluation Criteria，简称TCSEC），以及该标准的可信数据库系统的解释（Trusted Database Interpretation，简称为TDI），从而形成了最早的信息安全及数据库安全评估体系。TCSEC/TDI将系统安全性分为4组7个等级，依次是D（最小保护）、C1（自主安全保护）、C2（受控存取保护）、B1（标记安全保护）、B2（结构化保护）、B3（安全域）和A1（验证设计），按系统可靠或可信程度逐渐增高。

90年代后期，《信息技术安全评价通用准则》（Common Criteria，简称为CC）被ISO接受为国际标准，确立了现代信息安全标准的框架，这些标准指导了安全数据库系统的研究及其应用系统的开发。

在安全数据库需求及信息安全标准的推动下，国外各大主流数据库厂商相继推出了各自的安全数据库产品，如Sybase公司的Secure SQL Server（最早通过B1级安全评估）、Oracle公司的Trusted Oracle 7和Informix公司的Informix-online/Secure 5.0等。近几年来，Oracle公司的Oracle 9i和Oracle 10g从用户认证、访问控制、加密存储和审计策略等方面进一步加强了安全控制功能。

我国从80年代开始进行数据库技术的研究和开发，从90年代初开始进行安全数据库理论的研究和实际系统的研制。2001年，中国军方提出了我国最早的数据库安全标准——《军用数据库安全评估准则》。2002年，公安部发布了公安部行业标准——GA/T 389-2002：《计算机信息系统安全等级保护/数据库管理系统技术要求》。

90年代以来，华中理工大学（现华中科技大学）、中国人民大学和东北大学等单位对数据库安全技术进行了研究和实践，并开发出了相应的安全数据库软件，如基本达到B1级安全要求的

DM3 数据库、COBASE（KingBase）数据库 2.0 可信版本及 OpenBase Secure 等。

2003 年，中科院信息安全国家重点实验室基于开放源代码的数据库管理系统 Postgre SQL 开发出安全数据库系统 LOIS。

总体来说，与国外主流数据库产品相比，我国的研究成果在安全性和可用性上还有一定的差距。

根据 2004 年底的统计，几大国外数据库管理系统在国内的市场占有率达到 95%，国产数据库的总市场容量大约为 3.5%，其他开源的产品大约占 1.5%。国外的数据库产品不提供源程序代码，也很少有可供公开调用的内核接口，从而加大了自主安全保护的技术难度。加之发达国家限制 C2 级以上安全级别的信息技术与产品对我国的出口，所以研究开发数据库安全控制技术具有重要的现实意义，任重而道远。

1.1.2 数据库系统的安全需求

与其他计算机系统（如操作系统）的安全需求类似，数据库系统的安全需求可以归纳为完整性、保密性和可用性 3 个方面。

1. 完整性

数据库系统的完整性主要包括物理完整性和逻辑完整性。

物理完整性是指保证数据库的数据不受物理故障（如硬件故障或掉电等）的影响，并有可能在灾难性毁坏时重建和恢复数据库。

逻辑完整性是指对数据库逻辑结构的保护包括数据语义与操作完整性，前者主要指数据存取在逻辑上满足完整性约束；后者主要指在并发事务中保证数据的逻辑一致性。

2. 保密性

数据库的保密性是指不允许未经授权的用户存取数据。一般要求对用户的身份进行标识与鉴别，并采取相应的存取控制策略以保证用户仅能访问授权数据，同一组数据的不同用户可以被赋予不同的存取权限。同时，还应能够对用户的访问操作进行跟踪和审计。此外，还应该控制用户通过推理方式从经过授权的已知数据获取未经授权的数据，造成信息泄露。

3. 可用性

数据库的可用性是指不应拒绝授权用户对数据库的正常操作，同时保证系统的运行效率并提供用户友好的人机交互。

一般而言，数据库的保密性和可用性是一对矛盾，对这一矛盾的分析与解决构成了数据库系统的安全模型和一系列安全机制的主要目标。

1.1.3 数据库系统的安全模型

安全模型也称为“策略表达模型”，它是一种抽象且独立于软件实现的概念模型，数据库系统的安全模型是用于精确描述数据库系统的安全需求和安全策略的有效方式。

从 70 年代开始，一系列数据库安全模型与原型系统得到研究。80 年代末开始，研究的重点集中于如何在数据库系统中实现多级安全。即如何将传统的关系数据库理论与多级安全模型相结合，建立多级安全数据库系统。到目前为止，先后提出的基于多级关系模型的数据库多级安全模型主要有 Bell-La Padula（简称为 BLP）、Biba、SeaView 和 Jajodia Sandhu（简称为 JS）模型等。

在多级安全模型中，客体（各种逻辑数据对象）被赋予不同的安全标记属性，或称为“密级”（security level）；主体（用户或用户进程）根据访问权限也被分配不同的许可级（clearance level）。

主体根据一定的安全规则访问客体，以保证系统的安全性和完整性。一般地，多级安全模型还能对系统内的信息流动进行控制。传统模式中关系的定义需要修改以支持多级关系，其中关系的完整性约束及关系操作也需要改进以保证安全性。因此，数据库系统的多级安全模型是以多级关系数据模型为基础的。

与传统关系数据模型类似，多级关系数据模型中的三要素为多级关系、多级关系完整性约束和多级关系操作。此外，为解决实际存储问题，多级关系模型中还包括多级关系的分解与恢复算法。按由大到小的次序，多级访问控制粒度可分为关系级、元组级与属性级。粒度越小，则控制越灵活，相对应的多级关系模型越复杂。

随着研究的深入，人们逐渐认识到，多级安全模型与传统的关系数据库理论（如可串行化理论等）之间存在一定的内在冲突，导致在某些问题上必须在正确性与安全性之间妥协。比如，数据库多级安全模型通过引入多实例来解决数据完整性和推理控制问题。多实例不可避免地会带来数据一致性问题，也会影响系统的运行效率，在不少场合显得弊大于利。有的学者研究了消除多实例的方法，比如通过将所有的主键赋予可能的最低安全级来消除元组多实例的发生，但是这种方法大多限制了系统的可用性和灵活性。如何在满足数据的保密性和完整性的同时兼顾系统的可用性，这一直是数据库安全模型研究需要解决的一个重要问题。

1.1.4 数据库系统安全机制

数据库安全机制是用于实现数据库的各种安全策略的功能集合，正是由这些安全机制来实现安全模型，进而实现保护数据库系统安全的目标。近年来，对用户的认证与鉴别、存取控制、数据库加密及推理控制等安全机制的研究取得了不少新的进展。

1.1.4.1 用户标识与鉴别

用户标识是指用户向系统出示自己的身份证明，最简单的方法是输入用户 ID 和密码。标识机制用于惟一标志进入系统的每个用户的身份，因此必须保证标识的惟一性。鉴别是指系统检查验证用户的身份证明，用于检验用户身份的合法性。标识和鉴别功能保证了只有合法的用户才能存取系统中的资源。

由于数据库用户的安全等级是不同的，因此分配给他们的权限也是不一样的，数据库系统必须建立严格的用户认证机制。身份的标识和鉴别是 DBMS 对访问者授权的前提，并且通过审计机制使 DBMS 保留追究用户行为责任的能力。功能完善的标识与鉴别机制也是访问控制机制有效实施的基础，特别是在一个开放的多用户系统的网络环境中，识别与鉴别用户是构筑 DBMS 安全防线的第 1 个重要环节。

近年来标识与鉴别技术发展迅速，一些实体认证的新技术在数据库系统集成中得到应用。目前，常用的方法有通行字认证、数字证书认证、智能卡认证和个人特征识别等。

通行字也称为“口令”或“密码”，它是一种根据已知事物验证身份的方法，也是一种最广泛研究和使用的身份验证法。在数据库系统中往往对通行字采取一些控制措施，常见的有最小长度限制、次数限定、选择字符、有效期、双通行字和封锁用户系统等。一般还需考虑通行字的分配和管理，以及在计算机中的安全存储。通行字多以加密形式存储，攻击者要得到通行字，必须知道加密算法和密钥。算法可能是公开的，但密钥应该是秘密的。也有的系统存储通行字的单向 Hash 值，攻击者即使得到密文也难以推出通行字的明文。

数字证书是认证中心颁发并进行数字签名的数字凭证，它实现实体身份的鉴别与认证、信息

完整性验证、机密性和不可否认性等安全服务。数字证书可用来证明实体所宣称的身份与其持有的公钥的匹配关系，使得实体的身份与证书中的公钥相互绑定。

智能卡（有源卡、IC 卡或 Smart 卡）作为个人所有物，可以用来验证个人身份，典型智能卡主要由微处理器、存储器、输入输出接口、安全逻辑及运算处理器等组成。在智能卡中引入了认证的概念，认证是智能卡和应用终端之间通过相应的认证过程来相互确认合法性。在卡和接口设备之间只有相互认证之后才能进行数据的读写操作，目的在于防止伪造应用终端及相应的智能卡。

根据被授权用户的个人特征来进行确证是一种可信度更高的验证方法，个人特征识别应用了生物统计学（Biometrics）的研究成果，即利用个人具有惟一性的生理特征来实现。个人特征都具有因人而异和随身携带的特点，不会丢失并且难以伪造，非常适合于个人身份认证。目前已得到应用的个人生理特征包括指纹、语音声纹（voice- print）、DNA、视网膜、虹膜、脸型和手型等。一些学者已开始研究基于用户个人行为方式的身份识别技术，如用户写签名和敲击键盘的方式等。

个人特征一般需要应用多媒体数据存储技术来建立档案，相应地需要基于多媒体数据的压缩、存储和检索等技术作为支撑。目前已有不少基于个人特征识别的身份认证系统成功地投入应用。如美国联邦调查局（FBI）成功地将小波理论应用于压缩和识别指纹图样，从而可以将一个 10 MB 的指纹图样压缩成 500 KB，从而大大减少了数百万指纹档案的存储空间和检索时间。

1.1.4.2 存取控制

访问控制的目的是确保用户对数据库只能进行经过授权的有关操作。在存取控制机制中，一般把被访问的资源称为“客体”，把以用户名义进行资源访问的进程、事务等实体称为“主体”。

传统的存取控制机制有两种，即 DAC（Discretionary Access Control，自主存取控制）和 MAC（Mandatory Access Control，强制存取控制）。在 DAC 机制中，用户对不同的数据对象有不同的存取权限，而且还可以将其拥有的存取权限转授给其他用户。DAC 访问控制完全基于访问者和对象的身份；MAC 机制对于不同类型的信息采取不同层次的安全策略，对不同类型的数据来进行访问授权。在 MAC 机制中，存取权限不可以转授，所有用户必须遵守由数据库管理员建立的安全规则，其中最基本的规则为“向下读取，向上写入”。显然，与 DAC 相比，MAC 机制比较严格。

近年来，RBAC（Role-based Access Control，基于角色的存取控制）得到了广泛的关注。RBAC 在主体和权限之间增加了一个中间桥梁——角色。权限被授予角色，而管理员通过指定用户为特定角色来为用户授权。从而大大简化了授权管理，具有强大的可操作性和可管理性。角色可以根据组织中的不同工作创建，然后根据用户的责任和资格分配角色，用户可以轻松地进行角色转换。而随着新应用和新系统的增加，角色可以分配更多的权限，也可以根据需要撤销相应的权限。

RBAC 核心模型包含了 5 个基本的静态集合，即用户集（users）、角色集（roles）、特权集（perms）（包括对象集（objects）和操作集（operators）），以及一个运行过程中动态维护的集合，即会话集（sessions），如图 1-1 所示。

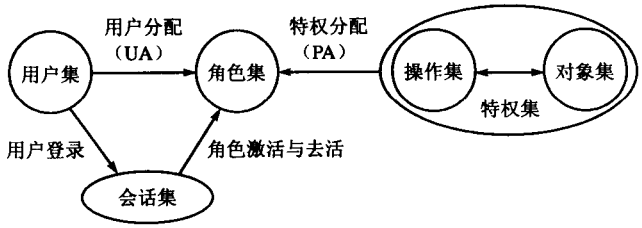

图 1-1 RBAC 核心模型

用户集包括系统中可以执行操作的用户，是主动的实体；对象集是系统中被动的实体，包含系统需要保护的信息；操作集是定义在对象上的一组操作，对象上的一组操作构成了一个特权；角色则是RBAC模型的核心，通过用户分配（UA）和特权分配（PA）使用户与特权关联起来。

RBAC属于策略中立型的存取控制模型，既可以实现自主存取控制策略，又可以实现强制存取控制策略。它可以有效缓解传统安全管理处理瓶颈问题，被认为是一种普遍适用的访问控制模型，尤其适用于大型组织的有效的访问控制机制。

2002年，Park. J和Sundhu. R首次提出了UCON（Usage Control，使用控制）的概念。UCON对传统的存取控制进行了扩展，定义了授权（Authorization）、职责（Obligation）和条件（Condition）3个决定性因素，同时提出了存取控制的连续性（Continuity）和易变性（Mutability）两个重要属性。UCON集合了传统的访问控制、可信管理，以及数字权力管理，从而用系统方式提供了一个保护数字资源的统一标准的框架，为下一代存取控制机制提供了新思路。

1.1.4.3 数据库加密

由于数据库在操作系统中以文件形式管理，所以入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者篡改数据库文件内容。另一方面，数据库管理员（DBA）可以任意访问所有数据，往往超出了其职责范围，同样造成安全隐患。因此，数据库的保密问题不仅包括在传输过程中采用加密保护和控制非法访问，还包括对存储的敏感数据进行加密保护，使得即使数据不幸泄露或者丢失，也难以造成泄密。同时，数据库加密可以由用户用自己的密钥加密自己的敏感信息，而不需要了解数据内容的数据库管理员无法进行正常解密，从而可以实现个性化的用户隐私保护。

对数据库加密必然会带来数据存储与索引、密钥分配和管理等一系列问题，同时加密也会显著地降低数据库的访问与运行效率。保密性与可用性之间不可避免地存在冲突，需要妥善解决二者之间的矛盾。

数据库中存储密文数据后，如何进行高效查询成为一个重要的问题。查询语句一般不可以直接运用到密文数据库的查询过程中，一般的方法是首先解密加密数据，然后查询解密数据。但由于要对整个数据库或数据表进行解密操作，因此开销巨大。在实际操作中需要通过有效的查询策略来直接执行密文查询或较小粒度的快速解密。

一般来说，一个好的数据库加密系统应该满足以下几个方面的要求。

① 足够的加密强度，保证长时间且大量数据不被破译。

② 加密后的数据库存储量没有明显的增加。

③ 加解密速度足够快，影响数据操作响应时间尽量短。

④ 加解密对数据库的合法用户操作（如数据的增、删、改等）是透明的。

⑤ 灵活的密钥管理机制，加解密密钥存储安全，使用方便可靠。

1. *数据库加密的实现机制*

数据库加密的实现机制主要研究执行加密部件在数据库系统中所处的层次和位置，通过对比各种体系结构的运行效率、可扩展性和安全性，以求得最佳的系统结构。

按照加密部件与数据库系统的不同关系，数据库加密机制可以从大的方面分为库内加密和库外加密。

（1）库内加密

库内加密在DBMS内核层实现加密，加/解密过程对用户与应用透明，数据在物理存取之前完成加/解密工作。