



数据库系统概论

An Introduction to Database System

第四章 数据库安全性

刘淇

Email: qiliuql@ustc.edu.cn

课程主页:

<http://staff.ustc.edu.cn/~qiliuql/DB2020HF.html>



复习：数据由DBMS统一管理和控制

2

□ DBMS提供的数据控制功能

□ (1)数据的安全性 (Security) 保护 (第4章)

保护数据，以防止不合法的使用造成的数据的泄密和破坏。

□ (2)数据的完整性 (Integrity) 检查 (第5章)

将数据控制在有效的范围内，或保证数据之间满足一定的关系。

□ (3)数据库恢复 (Recovery) (第10章)

将数据库从错误状态恢复到某一已知的正确状态。

□ (4)并发 (Concurrency) 控制 (第11章)

对多用户的并发操作加以控制和协调，防止相互干扰而得到错误的结果。



数据库安全性

3

- 问题的提出
 - 数据库的一大特点是数据可以共享
 - 数据共享必然带来数据库的安全性问题
 - 数据库系统中的数据共享不能是无条件的共享
- 例：军事秘密、国家机密、新产品实验数据、市场需求分析、市场营销策略、销售计划、客户档案、医疗档案、银行储蓄数据



数据库安全性



数据库安全性

4

- 对数据库安全性产生威胁的主要因素
- 非授权用户对数据库的恶意存取和破坏
- 数据库中重要或敏感的数据被泄露
- 安全环境的脆弱
 - 计算机硬件、操作系统、网络系统等



数据泄露、篡改的例子

5



MEGA上出现**7.73亿邮箱**和**2200万独立密码**

事件回顾：

2019年1月16日，安全研究专家Troy Hunt在博客中称，云存储服务平台MEGA上被黑客公开了窃取的7.73亿个电子邮件和近2200万个密码。总文件超过1.2万份，其中包含部分已”dehashed”的密码，数据超过87G，总共构成27亿个可用于撞库的攻击列表组合。外媒称其为“史上规模最大公共数据泄露事件”

The screenshot shows the MEGA interface with a sidebar containing various data collections like BTC combos, EU combos, Games combos, etc. The main area displays a list of files under 'NEW combo semi private > Dumps'. A context menu is open over one of the files, showing options like 'Info', 'Download...', 'Linkexport', and 'Import'. The table below lists the files with columns for Name, Größe (Size), Typ (Type), and Uploaddatum (Upload date). The data includes numerous websites and their associated file sizes and upload times.

Name	Größe	Typ	Uploaddatum
www.hundesalon-lili.at [56.463] [NOHASH].txt	1.8 MB	Text Document	2018-12-15 07:16
www.huntclublisting.com [13.857]	456 KB	Text Document	2018-12-15 07:16
www.hypnoseries.tv [102.497] [NOHASH].txt	2.9 MB	Text Document	2018-12-15 07:16
www.ias100.in [257.343] [NOHASH].txt	8.4 MB	Text Document	2018-12-15 07:16
www.icontrolpollution.com [44.94]	1.4 MB	Text Document	2018-12-15 07:16
www.immersionprograms.com [11]	379 KB	Text Document	2018-12-15 07:16
www.ineedtutor.ru [10.103] [NOHASH].txt	245 KB	Text Document	2018-12-15 07:16
www.innovationreview.eu [24.269]	720 KB	Text Document	2018-12-15 07:16
www.integrame.ro [31.232] [NOHASH].txt	1002 KB	Text Document	2018-12-15 07:16
www.interlinepublishing.com [8.126] [NOHASH].txt	259 KB	Text Document	2018-12-15 07:16
www.investingwithinsight.com [9.360] [NOHASH].txt	293 KB	Text Document	2018-12-15 07:16
www.iregisteredonline.com [9.166] [NOHASH].txt	292 KB	Text Document	2018-12-15 07:16
www.irg-listings.com [9.778] [NOHASH].txt	320 KB	Text Document	2018-12-15 07:16
www.islandpages.com [16.466] [NOHASH].txt	500 KB	Text Document	2018-12-15 07:16
www.italiansonline.net [170.663] [NOHASH].txt	5.2 MB	Text Document	2018-12-15 07:16
www.itotal.ru [508.490] [NOHASH].txt	13.0 MB	Text Document	2018-12-15 07:16
www.japanese-edu.org.hk [112.970] [NOHASH].txt	3.4 MB	Text Document	2018-12-15 07:16
www.kazachok.com [42.738] [NOHASH].txt	1.4 MB	Text Document	2018-12-15 07:16
www.kepzeslista.hu [11.543] [NOHASH].txt	343 KB	Text Document	2018-12-15 07:16
www.kesar.club [10.135] [NOHASH].txt	325 KB	Text Document	2018-12-15 07:16



数据泄露、篡改的例子

6



Facebook与逾150家公司分享数据，美检方展开刑事调查

事件回顾：

2019年3月13日，《纽约时报》报道称，Facebook因与其他科技公司签署数据共享协议而遭到美国司法部门的刑事调查。根据这些协议条款，Facebook 允许苹果、亚马逊和微软等设备制造商访问个人用户数据，包括好友列表、联系信息，甚至是私人信件，但并非所有访问都征得用户的同意。目前，至少有两家生产智能手机和其他电子设备的科技公司因该协议收到了纽约大陪审团的传票。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

7



5000万脸书用户的信息被泄漏并被非法利用

事件回顾：

2018年3月17日，据英国《观察家报》和《卫报》以及美国《纽约时报》报道，剑桥分析公司「窃取」5000万脸书用户的信息，是这家社交媒体创建以来最大的用户数据泄露事件之一。随后，Facebook迫于舆论压力，宣布暂时封杀两家关联机构。这次用户数据泄漏引发全球讨论，Facebook的CEO马克·扎克伯格也出席了美国参议院举行的2天10小时的听证会，接受44位参议员的轮番质询。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

8

2019年4月11日，厄瓜多尔总统宣布撤销对47岁的维基解密创始人朱利安-阿桑奇的政治庇护，随后阿桑奇立即遭到英国警方逮捕，至此结束了长达七年的庇护生活。



朱利安-阿桑奇，澳大利亚互联网积极分子，“维基解密”唯一公开身份的创始人，被称为“黑客罗宾汉”。他认为，公共治理机构的秘密文件和信息的透露，对大众来说是件有益的事。
9万份机密战争文件，揭开阿富汗战争杀戮平民的真相；**40万份**秘密战地记录，彻底曝光伊拉克战争虐囚罪恶；**25万份**美国外交电报，催生肯尼亚骚乱、突尼斯政变、埃及暴动……



数据泄露、篡改的例子

9



AcFun遭黑客攻击，近千万用户数据外泄

事件回顾：

2018年6月13日凌晨，AcFun(A站)发布公告称，A站受到黑客攻击，近千万条用户数据外泄。黑客攻击A站窃取的用户信息很快被放在暗网售卖，并喊出900万条用户数据，售价40万人民币，如果购买者对信息真实性质疑，那么可以随机抽取测试。其实早在今年3月份，暗网论坛中就有人公开出售AcFun的一手用户数据，数量高达800万条，而价格仅为12000元，平均1元能买到800条。





数据泄露、篡改的例子

10



10亿条圆通快递数据被公开叫卖

事件回顾：

2018年6月19日，一位ID为“f666666”的用户公然在暗网上兜售圆通10亿条快递数据，这引发了外界的广泛关注。据称，这些外泄的数据是2014年下旬的数据，其中包括有寄(收)件人姓名，电话，地址等信息。当时暗网对外泄数据进行了明码标价，用户只需花费430元人民币即可购买到100万条圆通快递的个人用户信息，而10亿条数据则需要约43000元人民币(约当时1比特币)。



圆通速递



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

11



万豪酒店数据库被入侵，**5亿用户核心信息遭窃**

事件回顾：

2018年11月底，万豪对外发出公告称旗下喜达屋酒店预订系统遭网络“黑客”入侵，自2014年起泄露大约5亿客户的用户信息。万豪泄露的这5亿用户信息中，包括用户的姓名、住址、电话号码、电子邮件地址、护照号码、信用卡等所有核心的信息，性质十分恶劣。美国诉讼集团代表众多消费者向万豪提起诉讼，索赔金额高达125亿美元。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

12

2018年信息泄露事件盘点

序号	涉事国家/企业	事件回顾	时间	数据规模
1	Facebook	剑桥分析未经用户许可，使用Facebook用户信息	2018.3	8700万用户信息
2	美国运动品牌Under Armour	旗下品牌因存在漏洞遭到黑客攻击用户信息泄露	2018.3	1.5亿用户信息，包括用户名、电子邮件、密码等
3	美国面包连锁店Panera Bread	未对漏洞进行及时修复，用户信息泄露	2018.4	3700万用户信息泄露，在官方公告前，泄露已超过8个月
4	基因检测网站MyHeritage	服务器遭到攻击，用户信息遭到截取	2018.6	9200万用户信息泄露
5	AcFun弹幕视频网	用户数据被窃取并公开贩卖	2018.6	900万条用户信息被窃取，并在暗网公开售卖，标价40万人民币
6	前程无忧	求职简历遭到泄露并贩卖	2018.6	195万用户求职简历遭到窃取，并在暗网贩卖
7	圆通速递	出售快递数据	2018.6	10亿条快递数据在暗网兜售，包含寄(收)件人姓名、电话、地址
8	华住旗下多个连锁酒店	用户私人信息泄露	2018.8	2.4亿入住记录、1.3亿条身份登记信息、1.23亿条官网注册信息
9	顺丰	用户信息被出售	2018.8	3亿用户信息被售卖2个比特币
10	万豪喜达屋	遭黑客入侵，用户信息被窃	2018.11	泄露5亿用户信息，包括护照号、信用卡等核心信息，性质恶劣



数据泄露、篡改的例子

13

2017年的数据泄漏事件涉及范围也很广泛，从单纯的社交网络拓展到了包括政府组织和知名企业在内的方方面面

2017年，IBM Security 和 Ponemon Institute两家研究机构针对419家公司进行调研，合计数据泄露总成本达到362万美元。每条包含敏感和机密信息的丢失或被盗记录的平均成本达到141美元。对比往年，今年企业和组织数据泄露的规模较以往更大，平均规模增长了1.8%。



数据泄露、篡改的例子

14

2017年信息泄露事件盘点

序号	涉事国家/企业	事件回顾	时间	数据规模
1	美国国防部AWS S3服务器	泄露18亿条公民信息	2017.11	18亿条来自社交媒体和论坛的帖子
2	南非金融信贷机构 TransUnion	用户数据被发布到一台完全未经保护的服务器	2017.10	3160万份用户的个人资料
3	马来西亚	用户手机号外泄	2017.10	约4620万份手机用户资料
4	Instagram	安全漏洞被恶意代码利用窃取用户的账户信息	2017.9	600万名人 Instagram 账户的邮件地址和电话号码
5	美国信用机构 Equifax	遭到黑客袭击，大量用户数据泄露	2017.9	1.43亿名用户数据
6	Verizon 公司	存储实例没有得到充分的保护，数据遭到泄漏	2017.7	1400万 Verizon 客户个人数据
7	美国 Deep Robot Analytics	将近2亿人的投票信息泄露	2017.6	1.98亿美国选民的个人信息
8	Edmodo 教育平台	黑客入侵 Edmodo 教育平台窃取账户信息	2017.6	数千万用户账户信息（用户名、电子邮箱地址以及密码等）
9	商业信息服务机构 Dun&Bradstreet	独有电子邮件地址和联系信息曝光	2017.3	近3370万用户电子邮件地址和联系信息
10	以色列执法机构 Cellebrite	遭到黑客入侵，致使大量内部机密文件被盗	2017.1	900GB的内部机密文件



数据泄露、篡改的例子

15



600万名人Instagram账户邮件地址和电话号码遭泄漏

事件回顾：

2017年9月，黑客利用图片社交应用Instagram应用程序界面存在的安全漏洞，通过恶意代码窃取到用户的账户信息。虽然该漏洞已被修复，但该事件的影响力远比想象中严重。在此次恶意攻击中，黑客宣称窃取了包括大量娱乐、体育明星在内的600万名人Instagram账户的邮件地址和电话号码。窃取信息成功的黑客还建立了一个名为“Doxagram”的数据库，任何人只要付费10美元，即可在数据库中查询到相关名人的隐私信息。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

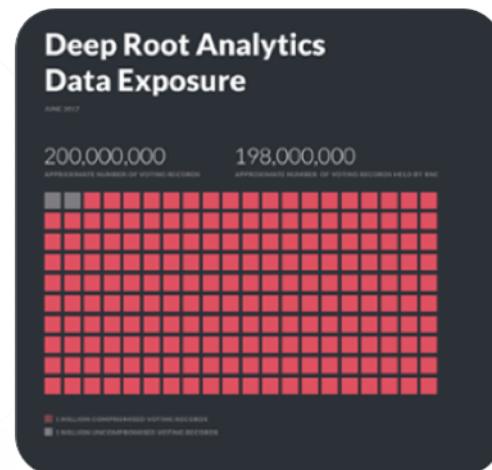
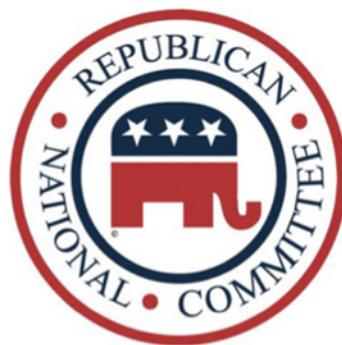
16



1.98亿美国选民的个人信息被公开

事件回顾：

2017年6月，安全研究人员发现有将近2亿人的投票信息泄露，主要是由于美国共和党全国委员会的承包商Deep Root Analytics误配置数据库所导致，这些数据保存在了一个可公开访问的云服务器上，托管在亚马逊的AWS S3云服务器中。泄露的1.1TB数据包含超过1.98亿美国选民的个人信息，姓名、出生日期、家庭地址、电话号码、选民登记详情等。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

17



超过1亿条优酷账户信息数据库在暗网售卖

事件回顾：

2017年4月17日，外国媒体hackread报道，100759591条优酷账户信息数据库在暗网售卖，该数据库售卖价格定为0.2559比特币，折合人民币约2065.56元。与此同时，同一暗网市场有卖家正在售卖2100万Gmail和Yahoo账号、64万解密PlayStation账号、11个被黑比特币网站的数百万账号，以及25个被入侵vBulletin论坛的数百万账号。

The screenshot shows a listing for a Youku account database from 2016. The title is "100.759.591 Youku Leaked Database 2016 [Cheap] & [Highly Private]". The price is listed as "USD 300.48 (including 0.48 transaction fee)" and "0.2480 Bitcoin". A "Buy Now" button is visible. Below the main title, there are vendor details: "cosmidark [+14]", "Level 8 (50)", "Physical", "Ships From Worldwide", and "Ships To Worldwide". At the bottom, there are links for "youku.pw", "youku.vbulletin", "youku.vbulletin", and "youku.vbulletin".

An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

18



利用漏洞肆意篡改成绩 软件开发人员获刑

事件回顾：

2017年5月2日，沈阳某高校报案称，该校的成绩管理系统被他人恶意攻击，数十名在校学生的考试成绩被篡改，导致毕业学生成绩无法进行有效确认。经过对受入侵系统服务器的大量数据进行核查、分析，最终锁定并抓获了曾就职于开发该高校成绩管理系统的张某某。经审讯，该人利用曾参与该高校计算机成绩管理系统软件开发之便，以每科300元的价格为该校学生修改考试成绩，期间非法获利4万余元。





数据泄露、篡改的例子

19

2016年十大数据泄露事件 社交网络成泄露重灾区

据日前Gemalto曝出的数据
显示：2016年上半年的数据泄露
总数增长了15%。
在全球范围内，2016年上半年已曝光的数据泄露事件高达
974起，数据泄露记录总数超过了5.54亿条之多。

2016年十大数据泄露事件				
序号	涉及国家/企业	时间	用户及账号规模	
1	TIME WARNER CABLE 美国·时代华纳	2016/1	32万	
2	土耳其政府	2016/4	5000万	
3	tumblr. 美国.Tumblr	2016/5	6500万+	
4	LinkedIn 美国.LinkedIn	2016/5	1.67亿	
5	YAHOO! Google 美国. Microsoft 谷歌、雅虎、微软等	2016/5	2.723亿	
6	myspace® 美国. MySpace	2016/6	4.27亿	
7	WORLD-CHECK 英国. 反恐资料库 WorldCheck	2016/6	220万	
8	美国. 国家安全局	2016/8	不详	
9	YAHOO! 美国.雅虎	2016/9	5亿	
10	网易 NETEASE www-163.com 中国.网易	2016/10	1亿+	

制榜：数据猿



数据泄露、篡改的例子

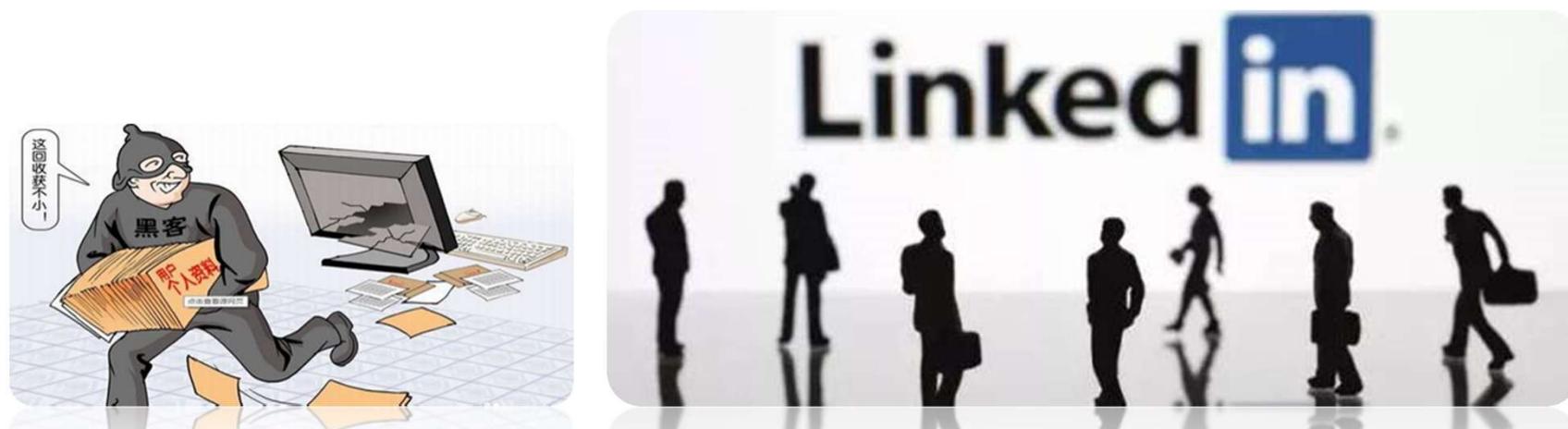
20



LinkedIn 超1.67亿个账户在黑市被公开销售

事件回顾：

2016年5月19日，美国职业社交网站LinkedIn宣布，有一名叫“peace”的黑客组织在黑市上以5比特币(约合2200美元)的售价公开销售1.67亿个领英用户登录信息。据了解，这些数据来自于2012年LinkedIn发生的一次大范围的数据泄露事件，其中有1.17亿既包括电子邮件，也包括密码。当时公司方面曾花费100万美元展开调查，但未真正意识到问题的严重性，才在几年之后造成如此恶劣影响。





数据泄露、篡改的例子

21



2.723亿电子邮箱信息以1美元价格流入黑市

事件回顾：

2016年5月，一名俄罗斯黑客盗取了2.723亿电子邮箱信息，其中包括4000万个雅虎邮箱、3300万微软邮箱以及2400万个谷歌邮箱。之后这些信息流入俄罗斯黑市，并以不到1美元的价格进行出售。





数据泄露、篡改的例子

22



世界最大反恐数据库在暗网出售，卖家称数据真实有效

事件回顾：

2016年6月，世界最大的反恐资料库WorldCheck资料曾外泄，**220万个可疑恐怖分子和与犯罪组织有关的人员**的个人资料在网上出现，不但如此，这些数据还分别以**3.5比特币(2345美元)**以及**10比特币(6706美元)**的售价在暗网公开售卖。

根据售卖列表可以分析出，这次的始作俑者是名为DataDirect和BestBuy的两名黑客。经事后了解，该数据库出现问题的主要原因是由于一台服务器(CouchDB)出现漏洞才导致其发生泄露。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

23



电脑工程师篡改数据 深圳3305万大奖是伪造

事件回顾：

2012年6月，省内各大媒体均发出“深圳3305万元双色球大奖急寻得主”的消息，指出如大奖得主7月9日之前不现身兑奖，这3305万元将成为当时国内最大金额的弃奖。

让人意想不到的是，7月8日，各大媒体都收到了深圳公安局发布的通稿：这5注头奖竟然是深圳一电脑工程师利用职务之便，通过木马程序，恶意篡改开奖后的彩票数据的结果，该工程师已被深圳警方抓获。



An Introduction to Database System



南方都市报
www.nddaily.com



漫画:邝斌
4/25/2020



数据泄露、篡改的例子

24



帮挂科大学生篡改成绩 四川“学霸”黑客获刑

事件回顾：

22岁的大学生小闫成绩优异，大一提前学完4年计算机课程，大三成为高级软件开发工程师，还曾获省级、全国级计算机类大奖。

然而，从2016年开始，他频繁入侵四川多家高校的教务系统，并通过QQ群、百度贴吧等平台招徕“生意”，以数百元不等的价格，替“挂科”学生篡改成绩，牟利达4.8万元。目前，小闫因破坏计算机信息系统罪，被判处有期徒刑五年。



An Introduction to Database System



4/25/2020



数据泄露、篡改的例子

25

2015年信息泄露事件盘点

序号	涉事国家/企业	事件回顾	账号规模
1	Topface (俄罗斯)	Topface泄露2000万用户数据	2000万
2	美国医疗保险公司	Anthem遭黑客攻击 8000万用户资料受影响	8000万
3	社保系统	社保系统被曝漏洞，个人信息泄露	5279.4万条
4	携程网	携程部分服务器遭到不明攻击宕机12小时	不详
5	HackingTeam (意大利)	HackingTeam被黑，“互联网军火”泄露	400GB
6	婚外情网站Ashley Madison (加拿大)	网站被黑 用户信息泄露	不详
7	大麦网	用户账号密码泄露 数据已被售卖	600多万
8	百利 (Experian)公司	电脑遭到黑客入侵，用户个人信息泄露	1500万
9	某电信系统	可以进行任意金额充值、销户、换卡	不详
10	伟易达Learning Lodge网站	客户资料外泄	500万



数据泄露、篡改的例子

26

2014年信息泄露事件盘点

序号	涉事国家/企业	事件回顾	账号规模
1	12306	用户账号串号，大量用户身份证等信息遭泄露	不详
2	支付宝	海量用户信息被非法买卖	超过20G
3	汉庭星空、浙江慧达	开房信息被泄漏	2000万
4	小米	系统漏洞导致用户资料大量泄漏	88W+360W
5	美国思科公司	路由器预置后门监控国民活动	不详
6	软件商“侵”车管所系统	非法删除14000余条交通违章记录	14000余条
7	某漏洞平台	漏洞导致考研用户的个人信息泄漏	130W
8	韩国	信用卡信息被泄露	2000万
9	土耳其	非法删除贫困地区巨额债务账单	约合65万美元



数据中的隐私泄露

27

The screenshot shows the Netflix Prize Leaderboard page. At the top, it says "COMPLETED". Below that, there's a blue banner with the text "被评选为09年IT行业100件最重要大事之一" (Selected as one of the top 100 most important events in the IT industry in 2009). The main table lists the top 10 teams with their scores, improvements, and submission times.

Rank	Team Name	Best Test Score	Improvement	Best Submit Time
1	Bellkor Predictor	0.9567	+0.04	2009-07-29 18:18:29
2	The Ensemble	0.9567	+0.04	2009-07-29 18:38:22
3	Ensemble Team	0.9562	+0.01	2009-07-19 21:24:49
4	Matrix Factorization	0.9560	+0.04	2009-07-18 01:12:21
5	Yannick's Submission	0.9561	+0.01	2009-07-18 00:12:29
6	François Fleuret	0.9564	+0.07	2009-09-24 12:05:59
7	Bellkor NoChill	0.9561	+0.01	2009-05-13 08:14:09
8	None...	0.9512	+0.00	2009-07-24 17:18:43



第四章 数据库安全性

28

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



4.1 计算机安全性概述

29

4.1.1 计算机系统的三类安全性问题

4.1.2 安全标准简介



4.1.1 计算机系统的三类安全性问题

30

- 计算机系统安全性
- 为计算机系统建立和采取的各种安全保护措施，以保护计算机系统中的硬件、软件及数据，防止其因偶然或恶意的原因使系统遭到破坏，数据遭到更改或泄露等。



计算机系统的三类安全性问题（续）

31

- 三类计算机系统安全性问题

- 技术安全类

- 管理安全类

- 政策法律类



4.1 计算机安全性概论

32

4.1.1 计算机系统的三类安全性问题

4.1.2 安全标准简介



4.1.2 安全标准简介

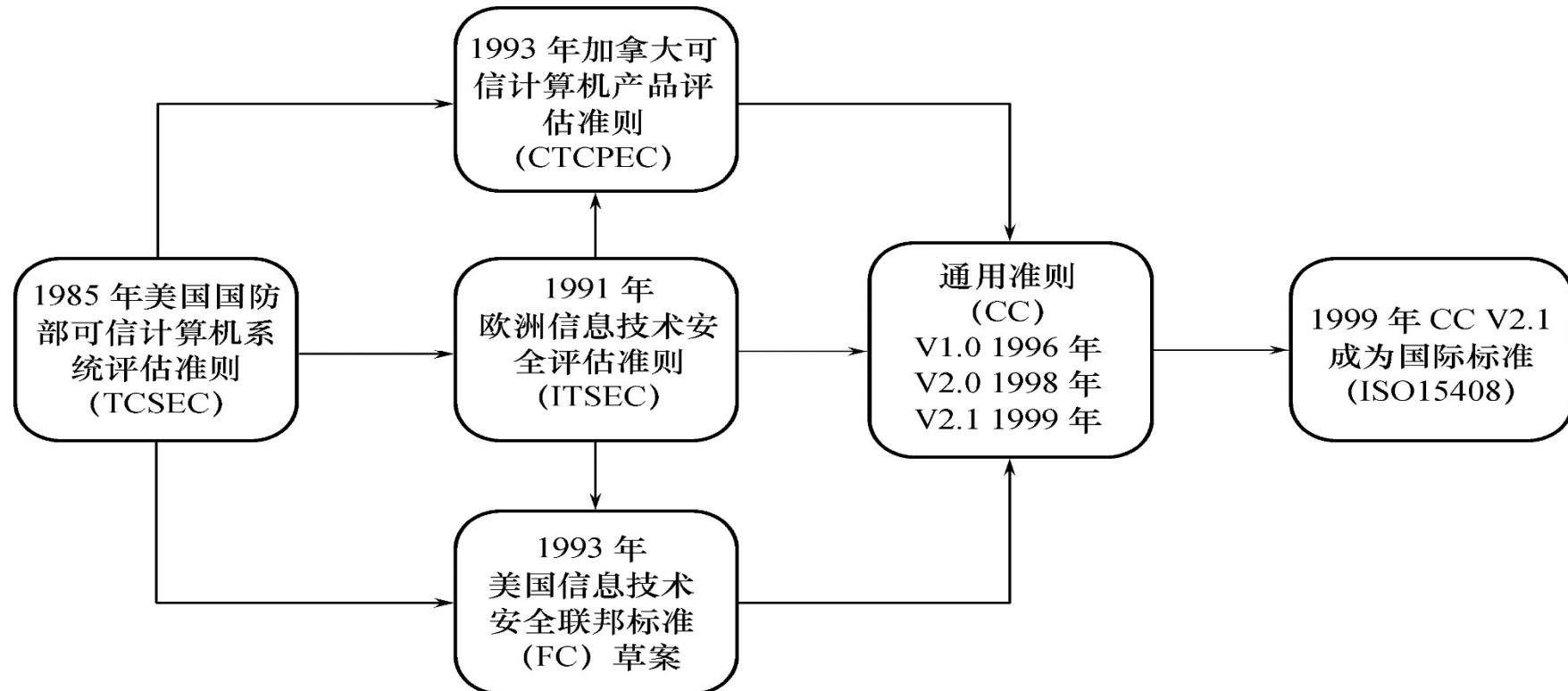
33

- TCSEC标准
 - 美国国防部可信计算机系统评估准则
 - 1985年颁布
- CC标准
 - 通用准则
 - 2001年成为我国标准



安全标准简介（续）

34



信息安全标准的发展历史



安全标准简介（续）

35

- TCSEC/TDI (Trusted Database Interpretation) 标准的基本内容
 - 可信计算机系统评估准则关于数据库系统的解释
 - TCSEC/TDI，从四个方面来描述安全性级别划分的指标
 - 安全策略
 - 责任
 - 保证
 - 文档



TCSEC/TDI安全级别划分

36

□ TCSEC/TDI安全级别划分

安全级别	定 义
A1	验证设计 (Verified Design)
B3	安全域 (Security Domains)
B2	结构化保护 (Structural Protection)
B1	标记安全保护 (Labeled Security Protection)
C2	受控的存取保护 (Controlled Access Protection)
C1	自主安全保护 (Discretionary Security Protection)
D	最小保护 (Minimal Protection)

按系统可靠或可信程度逐渐增高

各安全级别之间：偏序向下兼容

4/25/2020



TCSEC/TDI安全级别划分（续）

37

- B2以上的系统
- 还处于理论研究阶段
- 应用多限于一些特殊的部门，如军队等
- 美国正在大力发展安全产品，试图将目前仅限于少数领域应用的B2安全级别下放到商业应用中来，并逐步成为新的商业标准



CC

38

- CC (Common Criteria)
 - 提出国际公认的表述信息技术安全性的结构
 - 结构开放、表达方式通用
 - 把信息产品的安全要求分为
 - 安全功能要求
 - 信息技术的安全机制所要达到的功能和目的
 - 安全保证要求
 - 确保安全功能有效并正确实现的措施与手段



CC（续）

39

- CC文本组成
 - 简介和一般模型

- 介绍CC中有关的术语、基本概念和一般模型以及与评估有关的框架

- 安全功能要求
 - 列出了一系列类（11个）、子类（66个）和组件（135个）。
- 安全保证要求
 - 列出了保证类（11个）、子类（26个）和组件（74个），提出了评估保证级(EAL)



CC (续)

□ CC评估保证级划分

评估保证级	定 义	TCSEC安全级别（近似相当）
EAL1	功能测试 (functionally tested)	
EAL2	结构测试 (structurally tested)	C1
EAL3	系统地测试和检查 (methodically tested and checked)	C2
EAL4	系统地设计、测试和复查 (methodically designed, tested, and reviewed)	B1
EAL5	半形式化设计和测试 (semiformally designed and tested)	B2
EAL6	半形式化验证的设计和测试 (semiformally verified design and tested)	B3
EAL7	形式化验证的设计和测试 (formally verified design and tested)	A1



第四章 数据库安全性

41

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



4.2 数据库安全性控制概述

42

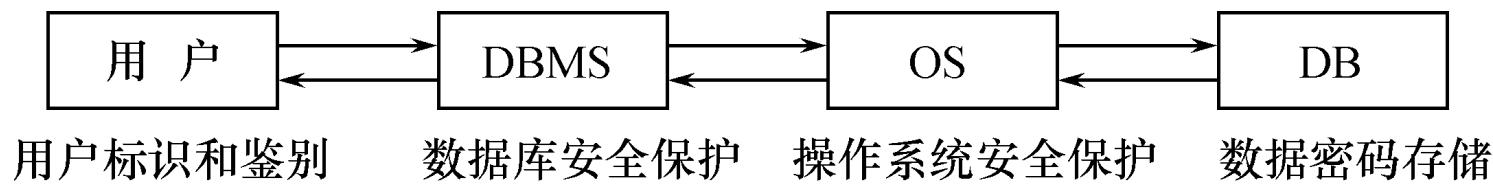
- 非法使用数据库的情况
 - 编写合法程序绕过DBMS及其授权机制
 - 直接或编写应用程序执行非授权操作
 - 通过多次合法查询数据库从中推导出一些保密数据



数据库安全性控制概述（续）

43

- 计算机系统中，安全措施一级一级层层设置



计算机系统的安全模型



数据库安全性控制概述（续）

44

□ 数据库安全性控制的常用方法

- 用户标识和鉴定
- 存取控制
- 视图
- 审计
- 密码存储



4.2 数据库安全性控制

45

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



4.2.1 用户标识与鉴别

46

- 用户标识与鉴别
(Identification & Authentication)
- 系统提供的最外层安全保护措施



用户标识与鉴别（续）

47

- 用户标识
- 口令
 - 系统核对口令以鉴别用户身份
- 用户名和口令易被窃取
 - 姓名、生日。 . .
 - 每个用户预先约定好一个计算过程或者函数



4.2 数据库安全性控制

48

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



4.2.2 存取控制

49

- 存取控制机制的组成
 - 定义用户权限
 - 合法权限检查
- 用户权限定义和合法权检查机制一起组成了 DBMS 的安全子系统



存取控制（续）

50

- 常用存取控制方法
 - 自主存取控制（Discretionary Access Control，简称DAC）
 - 用户可“自主”地决定将数据的存取权限授予何人、决定是否也将“授予”的权限授予别人
 - C2级
 - 灵活
 - 强制存取控制（Mandatory Access Control，简称MAC）
 - 系统“强制”地给用户和数据标记安全等级
 - B1级
 - 严格



4.2 数据库安全性控制

51

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



4.2.3 自主存取控制方法

52

- 通过 SQL 的 **GRANT** 语句和 **REVOKE** 语句实现
- 用户权限组成
 - 数据对象
 - 操作类型
- 定义用户存取权限：定义用户可以在哪些数据库对象上进行哪些类型的操作
- 定义存取权限称为**授权**



自主存取控制方法（续）

□ 关系数据库系统中存取控制对象

对象类型	对象	操作类型
数据库 模式	模式	CREATE SCHEMA
	基本表	CREATE TABLE, ALTER TABLE
	视图	CREATE VIEW
	索引	CREATE INDEX
数据 数据	基本表 和视图	SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALL PRIVILEGES
	属性列	SELECT, INSERT, UPDATE, REFERENCES ALL PRIVILEGES

在对用户授权列**INSERT**权限时，一定要包含对**主码**的**INSERT**权限，否则用户的插入会因为控制而被拒绝。**除了授权的列，其他列的值或者取空，或者取默认值。**

在对用户授权列**UPDATE**一列的权限时，用户修改该列仍然要遵守创建时定义的主码和其他约束。



4.2 数据库安全性控制

54

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



4.2.4 授权与回收

55

一、GRANT

- GRANT语句的一般格式：

GRANT <权限>[,<权限>]...

[ON <对象类型> <对象名>]

TO <用户>[,<用户>]...

[WITH GRANT OPTION];

- 语义：将对指定操作对象的指定操作权限授予指定的用户



GRANT (续)

56

□ 发出GRANT:

- DBA(数据库管理员, 类似于mysql中的root用户)
- 数据库对象创建者 (即属主Owner)
- 拥有该权限的用户

⑩ 接受权限的用户

- 一个或多个具体用户
- PUBLIC (全体用户)



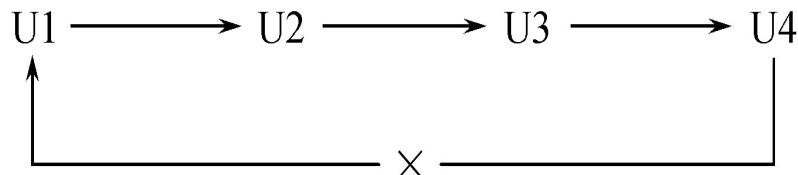
WITH GRANT OPTION子句

57

- WITH GRANT OPTION子句:

- 指定: 可以再授予
 - 没有指定: 不能传播

- 不允许循环授权





例题

58

[例1] 把查询Student表权限授给用户U1

```
GRANT SELECT  
ON TABLE Student  
TO U1;
```



例题（续）

59

[例2] 把对Student表和Course表的全部权限授予用户U2和U3

```
GRANT ALL PRIVILEGES  
ON TABLE Student, Course  
TO U2, U3;
```



例题（续）

60

[例3] 把对表SC的查询权限授予所有用户

```
GRANT SELECT  
ON TABLE SC  
TO PUBLIC;
```



例题（续）

61

[例4] 把查询Student表和修改学生学号的权限授给用户U4

```
GRANT UPDATE(Sno), SELECT  
ON TABLE Student  
TO U4;
```

- 对属性列的授权时必须明确指出相应属性列名



例题（续）

62

[例5] 把对表SC的INSERT权限授予U5用户，并允许他再将此权限授予其他用户

```
GRANT INSERT  
ON TABLE SC  
TO U5  
WITH GRANT OPTION;
```



传播权限

63

执行例5后，U5不仅拥有了对表SC的INSERT权限，
还可以传播此权限：

[例6] GRANT INSERT ON TABLE SC **TO U6**
WITH GRANT OPTION;

同样，U6还可以将此权限授予U7：

[例7] GRANT INSERT ON TABLE SC **TO U7;**
但U7不能再传播此权限。



传播权限（续）

下表是执行了〔例1〕到〔例7〕的语句后，学生-课程数据库中的用户权限
定义表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	PUBLIC	关系SC	SELECT	不能
DBA	U4	关系Student	SELECT	不能
DBA	U4	属性列 Student.Sno	UPDATE	不能
DBA	U5	关系SC	INSERT	能
U5	U6	关系SC	INSERT	能
U6	U7	关系SC	INSERT	不能



授权与回收（续）

65

二、REVOKE

- 授予的权限可以由DBA或其他授权者用REVOKE语句收回
- REVOKE语句的一般格式为：

REVOKE <权限>[,<权限>]...

[ON <对象类型> <对象名>]

FROM <用户>[,<用户>]...[CASCADE|RESTRICT];



REVOKE (续)

66

[例8] 把用户U4修改学生学号的权限收回

REVOKE UPDATE(Sno)

ON TABLE Student

FROM U4;



REVOKE (续)

67

[例9] 收回所有用户对表SC的查询权限

```
REVOKE SELECT  
ON TABLE SC  
FROM PUBLIC;
```



REVOKE (续)

68

[例10] 把用户U5对SC表的INSERT权限收回

```
REVOKE INSERT  
ON TABLE SC  
FROM U5 CASCADE;
```

- 将用户U5的INSERT权限收回的时候必须级联(CASCADE) 收回
- 系统只收回直接或间接从U5处获得的权限



REVOKE (续)

执行 [例8] 到 [例10] 的语句后，学生-课程数据库中的用户权限定义表

授权用户名	被授权用户名	数据库对象名	允许的操作类型	能否转授权
DBA	U1	关系Student	SELECT	不能
DBA	U2	关系Student	ALL	不能
DBA	U2	关系Course	ALL	不能
DBA	U3	关系Student	ALL	不能
DBA	U3	关系Course	ALL	不能
DBA	U4	关系Student	SELECT	不能



小结:SQL灵活的授权机制

70

- **DBA:** 拥有所有对象的所有权限
 - 不同的权限授予不同的用户
- **用户:** 拥有自己建立的对象的全部的操作权限
 - **GRANT:** 授予其他用户
- **被授权的用户**
 - “继续授权”许可: 再授予
- 所有授予出去的权力在必要时又都可用**REVOKE**语句收回



授权与回收（续）

三、创建数据库模式的权限

对创建数据库模式一类的数据库对象的授权

□ DBA在创建用户时实现

□ CREATE USER语句格式

CREATE USER <username>

[WITH] [DBA | RESOURCE | CONNECT]

[IDENTIFIED BY 'password'];



授权与回收（续）

拥有的权限	可否执行的操作			
	CREATE USER	CREATE SCHEMA	CREATE TABLE	登录数据库 执行数据查询和操纵
DBA	可以	可以	可以	可以
RESOURCE	不可以	不可以	可以	可以
CONNECT	不可以	不可以	不可以	可以，但必须拥有相应权限

权限与可执行的操作对照表



查询权限

- 查询某个用户的权限
 - `Show grants for USERNAME;`
 - `select * from mysql.user where user= USERNAME;`
- 查询所有用户
 - `select * from mysql.user` # myysql数据库中的用户表
- 查询针对不同对象具有操作权限的用户
 - 数据库级别的权限信息是mysql.db表
 - 表对象的授权信息记录是mysql.tables_priv表
 - 列级权限记录在mysql.column_priv表



选择题

74

SQL语言的GRANT和REVOKE语句主要是用来维护数据库的（ ）。

- A. 完整性
- B. 可靠性
- C. 安全性
- D. 一致性



选择题

75

SQL的GRANT和REVOKE语句可以用来实现（）

- A. 自主存取控制
- B. 强制存取控制
- C. 数据库角色创建
- D. 数据库审计



选择题

76

(多选题) 在对用户授权列**INSERT**权限时，一定要包含对（ ）的**INSERT**权限，否则用户的插入会因为控制而被拒绝。除了授权的列，其他列的值或者取（ ），或者取（ ）。

A. 主码

B. 外键

C. 空值

D. 默认值



4.2 数据库安全性控制

77

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



4.2.5 数据库角色

78

- 数据库角色：被命名的一组与数据库操作相关的权限
- 角色是权限的集合
- 可以为一组具有相同权限的用户创建一个角色
- 简化授权的过程



数据库角色

79

- 一、角色的创建

CREATE ROLE <角色名>

- 二、给角色授权

GRANT <权限> [, <权限>] ...

ON <对象类型>对象名

TO <角色> [, <角色>] ...



数据库角色

80

- 三、将一个角色授予其他的角色或用户

**GRANT <角色1> [, <角色2>] ...
TO <角色3> [, <用户1>] ...
[WITH ADMIN OPTION]**

WITH ADMIN OPTION--获得某种权限的角色或用户可以把这种权限再授予其他角色

- 四、角色权限的收回

**REVOKE <权限> [, <权限>] ...
ON <对象类型> <对象名>
FROM <角色> [, <角色>] ...**



数据库角色（续）

81

[例11] 通过角色来实现将一组权限授予一个用户。

步骤如下：

1. 首先创建一个角色 R1

CREATE ROLE R1;

2. 然后使用**GRANT**语句，使角色R1拥有**Student**表的
SELECT、UPDATE、INSERT权限。

GRANT SELECT, UPDATE, INSERT

ON TABLE Student

TO R1;



数据库角色（续）

82

3. 将这个角色授予王平，张明，赵玲。使他们具有角色R1所包含的全部权限

GRANT R1

TO 王平, 张明, 赵玲;

4. 可以一次性通过R1来回收王平的这3个权限

REVOKE R1

FROM 王平;



数据库角色（续）

83

[例12] 角色的权限修改

```
GRANT DELETE  
ON TABLE Student  
TO R1
```



数据库角色（续）

84

[例13]

```
REVOKE SELECT  
ON TABLE Student  
FROM R1;
```



4.2 数据库安全性控制

85

4.2.1 用户标识与鉴别

4.2.2 存取控制

4.2.3 自主存取控制方法

4.2.4 授权与回收

4.2.5 数据库角色

4.2.6 强制存取控制方法



存取控制

86

- 常用存取控制方法
 - 自主存取控制（Discretionary Access Control，简称DAC）
 - 用户可“自主”地决定将数据的存取权限授予何人、决定是否也将“授予”的权限授予别人
 - C2级
 - 灵活
 - 强制存取控制（Mandatory Access Control，简称MAC）
 - 系统“强制”地给用户和数据标记安全等级
 - B1级
 - 严格



自主存取控制缺点

87

- 可能存在数据的“无意泄露”
- 原因：这种机制仅仅通过对数据的存取权限来进行安全控制，而数据本身并无安全性标记
- 解决：对系统控制下的所有主客体实施强制存取控制策略



4.2.6 强制存取控制方法

88

- 强制存取控制（MAC）
 - 保证更高程度的安全性
 - 用户不能直接感知或进行控制
 - 适用于对数据有严格而固定密级分类的部门
 - 军事部门
 - 政府部门



强制存取控制方法（续）

89

- **主体**是系统中的活动实体
 - DBMS所管理的实际用户
 - 代表用户的各进程

- **客体**是系统中的被动实体，是受主体操纵的
 - 文件
 - 基表
 - 索引
 - 视图



强制存取控制方法（续）

90

- 敏感度标记（Label）
 - 绝密（Top Secret）
 - 机密（Secret）
 - 可信（Confidential）
 - 公开（Public）
- 主体的敏感度标记称为许可证级别（Clearance Level）
- 客体的敏感度标记称为密级（Classification Level）



强制存取控制方法（续）

91

□ 强制存取控制规则

(1) 仅当主体的许可证级别大于或等于客体的密级时，
该主体才能读取相应的客体

(2) 仅当主体的许可证级别小于或等于客体的密级时，
该主体才能写相应的客体

□ 修正（即）规则

□ 主体的许可证级别 \leq 客体的密级 \rightarrow 主体能写客体



强制存取控制方法（续）

92

□ 规则的共同点

禁止了拥有高许可证级别的主体更新低密级的数据对象



MAC与DAC

93

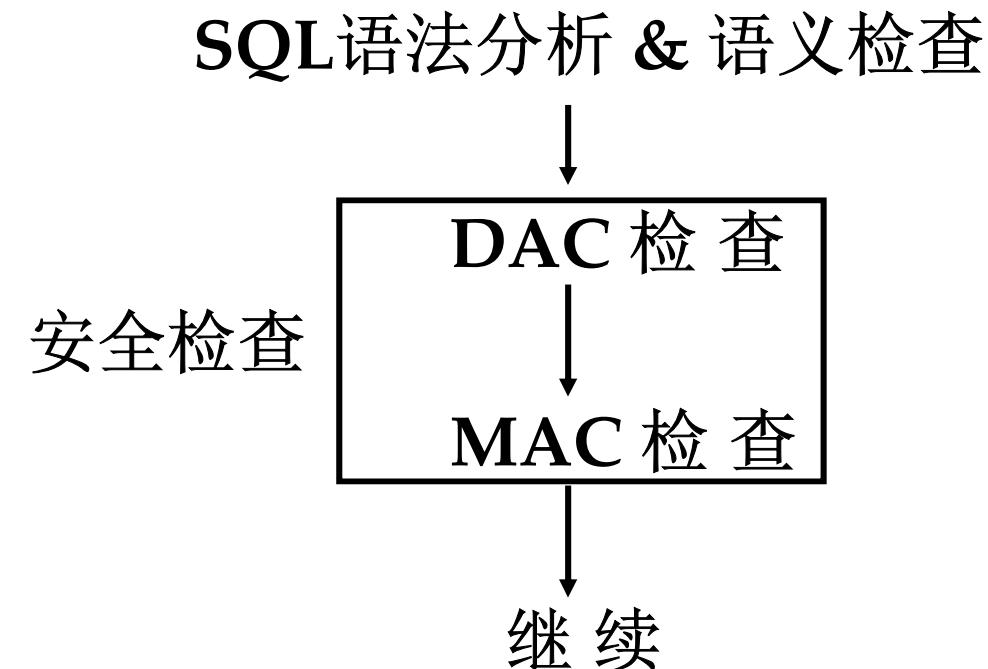
- DAC与MAC共同构成DBMS的安全机制
- 实现MAC时要首先实现DAC
 - 原因：较高安全性级别提供的安全保护要包含较低级别的所有保护



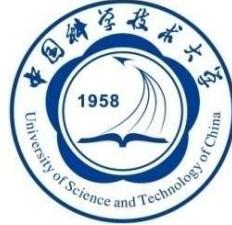
强制存取控制方法（续）

94

DAC + MAC安全检查示意图



- ❖ 先进行DAC检查，通过DAC检查的数据对象再由系统进行MAC检查，只有通过MAC检查的数据对象方可存取。



第四章 数据库安全性

95

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



4.3 视图机制

96

- 把要保密的数据对无权存取这些数据的用户隐藏起来，
对数据提供一定程度的安全保护
- 主要功能是提供数据独立性，无法完全满足要求
- 间接实现了支持存取谓词的用户权限定义



视图机制（续）

97

[例14]建立计算机系学生的视图，把对该视图的SELECT权限授于王平，把该视图上的所有操作权限授于张明

先建立计算机系学生的视图CS_Student

```
CREATE VIEW CS_Student  
AS  
SELECT *  
FROM Student  
WHERE Sdept='CS';
```



视图机制（续）

98

在视图上进一步定义存取权限

```
GRANT SELECT  
ON CS_Student  
TO 王平 ;
```

```
GRANT ALL PRIVILEGES  
ON CS_Student  
TO 张明;
```



4.2 数据库安全性控制

99

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



4.4 审计

100

□ 什么是审计

□ 审计日志（Audit Log）

将用户对数据库的所有操作记录在上面

□ DBA利用审计日志，找出非法存取数据的人、时间和内容

□ C2以上安全级别的DBMS必须具有



审计（续）

101

- 审计分为
 - 用户级审计
 - 针对自己创建的数据库表或视图进行审计
 - 记录所有用户对这些表或视图的一切成功和（或）不成功的访问要求以及各种类型的SQL操作
 - 系统级审计
 - DBA设置
 - 监测成功或失败的登录要求
 - 监测GRANT和REVOKE操作以及其他数据库级权限下的操作



审计（续）

102

- AUDIT语句：设置审计功能
- NOAUDIT语句：取消审计功能



审计（续）

103

[例15] 对修改SC表结构或修改SC表数据的操作进行审计

```
AUDIT ALTER, UPDATE  
ON SC;
```

[例16] 取消对SC表的一切审计

```
NOAUDIT ALTER, UPDATE  
ON SC;
```



4.2 数据库安全性控制

104

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

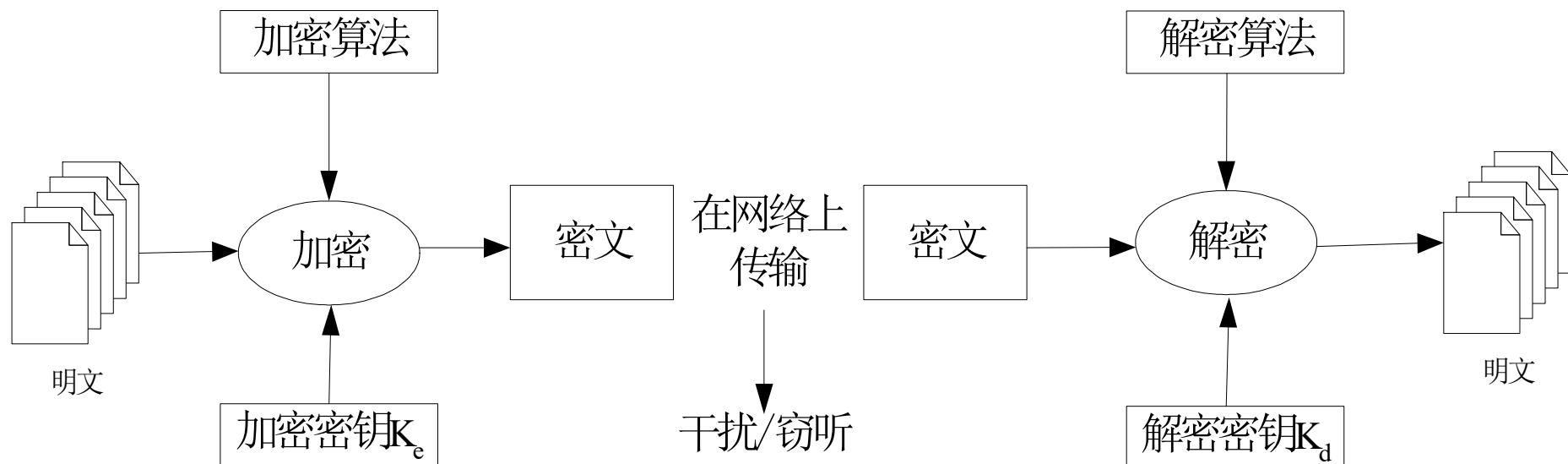
4.7 小结



4.5 数据加密

105

- 数据加密
- 防止数据库中数据在存储和传输中失密的有效手段





案例一

106

芦花丛中一扁舟，
俊杰俄从此地游，
义士若能知此理，
反躬逃难可无忧。

《水浒传》：吴用智赚玉麒麟

我画兰江水悠悠，
爱晚亭上枫叶稠，
秋月融融照佛寺，
香烟袅袅绕轻楼.

《唐寅诗集》



案例二

它是一种代换密码。据说凯撒是率先使用加密函的古代将领之一，因此这种加密方法被称为恺撒密码

密文: **jrg oryhv shrsoh**

算法: $C_i = E(P_i) = P_i + 3$ 恺撒密码

明文: **GOD LOVES PEOPLE**

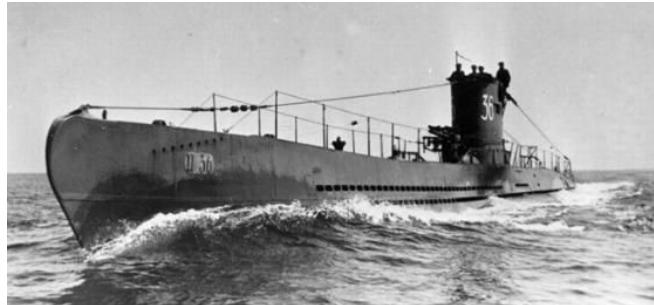
字母表: (密码本)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

d e f g h i j k l m n o p q r s t u v w x y z a b c



案例三



恩尼格玛密码机



1940年 英国 布莱切利园
BLETCHLEY PARK, ENGLAND - 1940



第四章 数据库安全性

109

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



其它安全性保护

110

- 推理控制
 - 避免用户利用其能访问的数据推知更高密级的数据
- 隐蔽信道
- 数据隐私保护
 - 控制不愿被他人知道或他人不便知道的个人数据的能力
 - 存在于数据生命周期的各个阶段



4.6 统计数据库安全性

111

- 统计数据库
 - 允许用户查询**聚集**类型的信息（如合计、平均值等）
 - 不允许查询**单个**记录信息
- 统计数据库中特殊的安全性问题
 - 隐蔽的信息通道
 - 能从合法的查询中推导出不合法的信息



统计数据库安全性（续）

112

规则1：任何查询至少要涉及N(N足够大)个以上的记录

规则2：任意两个查询的相交数据项不能超过M个

规则3：任一用户的查询次数不能超过 $1+(N-2)/M$



统计数据库安全性（续）

113

- 数据库安全机制的设计目标：

试图破坏安全的人所花费的代价 >> 得到的利益



第四章 数据库安全性

114

4.1 计算机安全性概述

4.2 数据库安全性控制

4.3 视图机制

4.4 审计 (Audit)

4.5 数据加密

4.6 其它安全性保护

4.7 小结



4.7 小结

115

- 数据的共享日益加强，数据的安全保密越来越重要
- DBMS是管理数据的核心，因而其自身必须具有一整套完整而有效的安全性机制
- TCSEC和CC



小结（续）

116

- 实现数据库系统安全性的技术和方法
 - 存取控制技术
 - 视图技术
 - 审计技术
- 自主存取控制功能
 - 通过SQL 的GRANT语句和REVOKE语句实现
- 角色
 - 使用角色来管理数据库权限可以简化授权过程
 - **CREATE ROLE**语句创建角色
 - **GRANT** 语句给角色授权