管理信息系统中的分级授权方案

李捷 徐嗣鑫 (南京东南大学自动化所 210096)

摘要:本文介绍了作者设计的一种管理信息系统中的分级动态授权方案。该方案将数据库授权和软件功能授权统一起来,提供简便的动态修改授权方案的途径、所有类型的软件模块入口的保护和分级管理机制,具有安全、可靠、简单和使用方便的特点,在江苏利港电力有限公司管理信息系统中得到了成功应用。

关键词:管理信息系统 安全性 授权 数据库

在 MIS 中,安全性是一个非常重要的方面。例如数据被不该知道的人知道,甚至被篡改或破坏,对系统的安全、正常运行造成了巨大威胁。因此,设计一个严密、合理、操作简单的授权机制是非常重要的。

作者设计了一种分级动态授权机制,并在江苏利港电力有限公司管理信息系统(以下简称利港 MIS)中得到了成功应用。该系统以 ORACLE 网络数据库为核心,以 DEVELOPER/2000 为主要开发工具,采用客户/服务器体系结构。

1. ORACLE 数据库的授权机制

数据库授权就是给予用户一定的访问特权,对用户对数据库数据的访问权限进行规定和限制。在 ORACLE 数据库中有两种授权:一种是授予某类数据库用户的特权,只有得到这种授权,才能成为数据库用户,这只能由 DBA 授予;另一种是授予对某些数据对象进行某些操作的特权,这可以由 DBA 授予,也可由数据对象创建者或具有转授权限的用户授予。

对于第一种授权,可用类似下面 SQL 语句:

GRANT〈特权类型〉TO〈用户标识符〉;

REVOKE〈特权类型〉FROM〈用户标识符〉;

特权类型为 CONNECT、RESOURCE 和 DBA;

第二种授权又可以分成两类,一是系统权限的授予,可用下面 SQL 语句:

GRANT〈系统权限〉TO〈用户标识符〉[WITH ADMIN OPTION];

REVOKE〈系统权限〉FROM〈用户标识符〉;

其中系统权限为 CREATE ANY TABLE、DROP ANY TABLE、GRANT ANY ROLE 等。

二是特定数据对象访问权限的授予,可用类似以下 SQL 语句:

GRANT〈特权〉ON〈表名〉TO〈用户标识符〉[WITH GRANT OPTION];

REVOKE〈特权〉ON〈表名〉FROM〈用户标识符〉;

其中特权可以为 ALTER、DELETE、EXECUTE、INDEX、INSERT、REFERENCES 和 UPDATE 等。

ORACLE 数据库本身的授权机制虽然很严格,但单纯依靠它并不能满足 MIS 对授权系统的要求,因为它只在数据库层次上为数据安全性提供保障,而且必须通过具体的授权指令来修改授权方案,因此必须在其基础上通过编程建立系统的授权机制。

2. 对授权方案的要求

根据对用户需求的调查和对实际系统的分析,授权方案应满足以下要求:

(1)系统的安全性包括两个方面:数据库数据对象的安全和软件功能的安全,软件功能的安全为数据库数据对象的安全提供保障,因此授权也必须包括两种:软件功能授权和数据库授权,而且必须将两者有机的结合起来。所谓数据库授权,就是对数据库访问权限的控制,也就是上文提到的 ORACLE 数据库的第二种授权;所谓软件功能授权,就是对使用软件模块权限的控制,只有获得软件功能授权的用户才能使用特定的软件模块。数据库授权在 DBMS 层次上为数据安全性提供保护,软件功能授权在应用层次上为数据安全性提供保护,二者是不可缺少的。数据库授权是保护数据安全性的最基本的手段,只有进行数据库授权才能在根本上保护数据的安全性;软件功能授权在更高层次上为数据的安全性提供保护,用户是通过软件对数据进行访问的,如果没有软件功能授权,不仅在逻辑上不合理,在实际中也会造成许多不可预料的错误。

(2)由于企业管理机制的改革和人员岗位职责的变化,对授权方案的修改是常见的,因此必须提供用户通过软件动态修改授权方案的途径,且操作要求相对简单,因

为这种操作是提供给管理人员使用的，而不是提供给技术人员使用的。

(3)由于系统的复杂性和方便用户操作，软件模块入口的类型是比较多的。为了确保系统的安全性，必须对软件模块的所有入口类型进行安全性保护，包括菜单项、导航按钮、功能按钮、触发器等。

(4)由于企业管理主要分成两级：部门级和公司级，因此授权机制也应分成两级：子系统授权和总授权。

3. 子系统授权的实现方法

子系统授权是指各子系统将子系统内部的软件功能模块和数据对象权限授予用户，是总授权的基础。我们首先介绍子系统授权的实现机制：

(1)为了将软件功能授权和数据库授权有机地结合起来，系统中应用了 ORACLE 数据库中角色的概念。所谓角色，实质上就是一系列数据库权限的集合。可以把数据库权限授予角色，再把角色授予用户。这里把每个软件功能模块所需要的所有数据库权限进行归纳总结并授予一个角色，当把这个软件功能模块的权限授予用户的同时，把此角色也授予用户。这样软件功能授权和数据库授权就有机的结合了起来。

例如利港 MIS 中的船舶动态表生成模块需要对船期预报和卸载情况两张基表的 SELECT 特权，可为其建立一个角色，命名为 LGMIS-R-RL 船舶动态表，表示其权限的 DDL 为：

GRANT SELECT ON 船期预报 TO LGMIS-R-RL 船舶动态表；

GRANT SELECT ON 卸载情况 TO LGMIS-R-RL 船舶动态表；

当把船舶动态表生成模块使用权限授予用户的同时，使用以下 DDL 语句所需的数据库权限也授予用户：

GRANT LGMIS-R-RL 船舶动态表 TO〈用户标识符〉；

这种权限管理的方法有如下的优点：

将软件功能管理和角色管理集成在一个系统中。授权工作由授权管理员统一完成，不会产生重复或不一致现象。授权时一方面将功能模块与其对应的应用角色联系起来，使用户能访问该功能模块；另一方面通过执行对应的 DDL 语句将角色授予用户，使其能访问该应用所需的数据对象，从而能真正使用该项功能。

其次，角色的划分是基于应用的，小粒度的。即开发人员是按照应用的功能而不是用户类型来划分角色。采用这种划分标准的原因在于：用户最终是通过执行应用程序来访问数据库；而且开发人员不应该静态地设定各类用户的角色而使其无法适应系统将来的变化。

第三，动态权限管理。由于每项应用功能所拥有的特权较少，因此角色的划分较为精细，从而减小了角色的粒度，给权限管理提供了充分的灵活性，系统安全员可以根据需要通过组合各功能模块来修改用户所拥有的权限，而无需修改应用程序。

(2)为了记录授权方案，需建立一个可命名为“授权”的基表，其建表 DDL 为：

CREATE TABLE 授权
(功能名 VARCHAR2(20),
用户名 VARCHAR2(12)；

其中功能名表示软件功能模块名，用户名表示拥有此软件功能模块使用权限的用户的用户名。由于利用角色的概念将软件功能授权和数据库授权结合了起来，这张表记录的既是软件功能授权的方案，同时也是数据库授权的方案。

(3)设计一个授权模块，授权模块完成的主要功能是查询“授权”表，确认用户具有哪些软件功能权限；由用户动态修改授权方案；根据修改后授权的方案通过 GRANT 或 REVOKE 语句将软件功能所对应的角色授予用户或从用户处收回；将修改后的授权方案存入“授权”表中。

在实际软件中采用了复选框来表示各软件模块的使用权限，授权管理员可先输入用户名，确认按钮完成用户已有权限的确认，若拥有某软件模块的使用权限则相应的复选框就会被选中，授权管理员通过修改复选框修改授权方案，授权按钮完成最终的授权。

图 1 为模块的程序流程图。

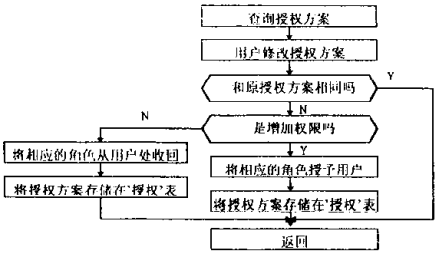

图 1　授权模块程序流程图

(4)在各软件功能模块的入口处嵌入判断代码，支持

已设定的授权方案。判断代码检索“授权”表，判断当前登录用户是否有权使用本模块，若有，则可正常进入，否则封锁此入口不允许进入。以下为利港 MIS 燃料子系统所使用的判断函数的 PL/SQL 代码。

```
function setmenu(menuname varchar2, func varchar2)
return number is
cursor c1 is select 用户名 from ranliao.授权 where 功能 = func;/ * 其他变量说明略 * /
begin / * menuname 为模块入口项，func 模块名，c1 为查询授权表的游标 * /
userstr: = GET-APPLICATION-PROPERTY ( username);/ * 取用户名 * /
open c1;
loop
fetch c1 into user;
exit when c1 % notfound;/ * 查用户是否有权限使用此模块 * /
if upper(user) = upper(userstr) then found: = 1; end if;
end loop;
close c1;
if found = 0 then / * 若无权限，封锁模块入口 * /
SET-MENU-ITEM-PROPERTY ( menuname, ENABLED, PROPERTY-FALSE);
elsif found = 1 then return(1); end if;
end;
```

4. 总授权的设计思想

总授权主要完成公司的高层管理人员对各子系统授权的控制，主要的功能是：

(1)为各子系统指定授权管理员。授权管理员拥有子系统授权模块的使用权限，负责各子系统授权工作。公司高层管理人员一般没有精力来管理各子系统内部的具体授权方案，但利用这个功能就可以通过指定子系统授权管理员来实现对子系统内部授权的控制。

(2)将各子系统所有功能统一授予用户。某些高层次用户往往需要某个子系统所有功能模块的使用权限，如果由子系统授权管理员逐一将各功能模块的使用权限授予，则相当烦琐，而通过这个功能就可以一次性将子系统所有功能统一授予用户，从而方便了用户。同时，这个功能也使得高层管理人员对各子系统内部授权有一个整体的控制。

功能(1)的设计思想是通过将各子系统内部授权模块的使用权限授予用户或从用户处收回来完成委任和撤消授权管理员的工作。功能(2)的实现思想将整个子系统看成是一个软件功能模块并将其需要的所有数据库权限归纳成一个角色，这样就可以使用授予功能模块使用权限同样的方法来完成子系统使用权限的授予。具体的实现方法和子系统授权的授权模块设计方法类似，这里不再详述。

5. 结论

该授权方案在江苏利港电力有限公司管理信息系统中得到了成功应用，事实证明它具有安全、可靠、简单和使用方便的特点，是一个很实用的授权方案。

参考文献

[1] 俞盘祥，《ORACLE 数据库系统基础》，清华大学出版社，1995 年 4 月

[2] 《ORACLE Developer/2000 使用技术与方法》(上、下册)，北京交通大学、自动化系统研究所 编著，1996 年 1 月

(来稿时间：1998 年 5 月)