Analysis Authorizations in BI - approach

The security concept in BI is different from that of a transaction system (ECC). In BI, the roles and authorizations are governed by reports and the ability to authorize the characteristics and key figures in those reports among users. So an effective authorization model in BI should take into account the following key concepts:

1. Adaptability for user creation of queries
2. Control data visibility at least along organizational data (eg: company, plant etc)
3. Provide a control Hierarchy for user access.

This blog will describe a matrix type strategy to configure a security model for a BI system. This is useful to retool existing security concepts to leverage the new analysis authorizations.

The new BI Analysis Authorizations use authorization objects created via transaction RSECADMIN to control access to characteristics that are authorization relevant. Those objects can be assigned via roles to users or directly to user ids. For this model I recommend controlling everything using roles instead of direct user assignment.

The two main types of roles for a BI Security concept would be:-

Reporting Roles: Roles that control access to Infoproviders and Queries/Workbooks.
Authorization Roles: Roles containing the relevant authorization objects.

The reporting roles will usually be sub divided based on the user access as super users and end users.

Super Users will have the following access:
1) Modify the Queries created by them.
2) Create, Change or Delete Workbooks under their corresponding roles.
3) Have access to all queries built under the Infoprovider assigned to them.

End User Access is follows:
1) Workbooks and Queries are display access only.
2) ‘n’ number of end user roles are created based on the number of queries accessible to end user groups.

Now let us consider an example to security model along these lines for two areas namely General Ledger(FI) and Inventory Management(IM). So the roles for this would be

General Ledger Accounting (FI -GL)

Super Role: GL_SUPERUSER (SGL)
End User Role: GL_ENDUSER(UGL)

Inventory Management

Super Role: IM_SUPERUSER(SIM)
End User Role: IM_ENDUSER(UIM)

Authorization Roles: For this model let us consider two authorization relevant organizational data characteristics for those areas (FI and IM) for sites 01 and 02.

0PLANT - Plant, 0COMPANY - Company Code

Hence for each characteristic a total of three authorization objects are created.

0PLANT:
PLANT00 - Auth object for all Plants
PLANT01 - Auth object for Plant 01
PLANT02 - Auth object for Plant 02

0COMPANY:
COMPANY00 - Auth object for all companies
COMPANY01 - Auth object for Company 01
COMPANY02 - Auth object for Company 02

The Authorization object is created in RSECADMIN as shown in Figure.
Authorization for PLANT01:

0PLANT is given the value 01.

0COMPANY is given an aggregated authorization. This is done so as to allow access to run queries having 0COMPANY as a value even though user restriction is based on 0PLANT.

Other Authorization relevant characteristics are maintained at full authorization.

Similarly other authorization objects are created. Each of the objects created is assigned to a role under object S_RS_AUTH.

The authorization roles will be as follows:

<table>
<thead>
<tr>
<th>Role</th>
<th>Auth. Obj.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROLE_PLANT_ALL</td>
<td>PLANT00</td>
</tr>
<tr>
<td>ROLE_PLANT_01</td>
<td>PLANT01</td>
</tr>
<tr>
<td>ROLE_PLANT_02</td>
<td>PLANT02</td>
</tr>
<tr>
<td>ROLE_COMP_ALL</td>
<td>COMPANY00</td>
</tr>
<tr>
<td>ROLE_COMP_01</td>
<td>COMPANY01</td>
</tr>
<tr>
<td>ROLE_COMP_02</td>
<td>COMPANY02</td>
</tr>
</tbody>
</table>

Role Matrix and User access:
The various types of users we may need to address are as follows:

User AS: Is a super user running reports for both GL and IM.

User AE: Is a end user running reports for both GL and IM.

User AS1: Is a super user for site 01 for both GL and IM.

User AE1: Is a end user for site 01 for both GL and IM.

User AS2: Is a super user for site 02 for both GL and IM.

User AE2: Is a end user for site 02 for both GL and IM.

User BS: Is a super user running reports for GL only.

User BE: Is a end user running reports for GL only.
User BS1: Is a super user for site 01 for GL.
User BE1: Is a end user for site 01 for GL.
User BS1: Is a super user for site 02 for GL.
User BE2: Is a end user for site 02 for GL.
User CS: Is a super user running reports for IM only.
User CE: Is a end user running reports for IM only.
User CS1: Is a super user for site 01 for IM.
User CE1: Is a end user for site 01 for IM.
User CS1: Is a super user for site 02 for IM.
User CE2: Is a end user for site 02 for IM.
User DS: Is a super user running GL reports for 01 and IM reports for 02.
User DE: Is a end user running GL reports for 01 and IM reports for 02.
User FS: Is a super user running GL reports for 02 and IM reports for 01.
User FE: Is a end user running GL reports for 02 and IM reports for 01.

The matrix for user to role assignment is now created with Auth.Roles in rows and Reporting Roles in columns as shown below:

<table>
<thead>
<tr>
<th>Auth/Reporting</th>
<th>SGL</th>
<th>UGL</th>
<th>SIM</th>
<th>UIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLANT00(All Plants)</td>
<td>AS</td>
<td>AE</td>
<td>AS,CS</td>
<td>AE,CE</td>
</tr>
<tr>
<td>PLANT01</td>
<td>AS1</td>
<td>AE1</td>
<td>AS1,CS1,FS</td>
<td>AE1,CE1,FE</td>
</tr>
<tr>
<td>PLANT02</td>
<td>AS2</td>
<td>AE2</td>
<td>AS2,CS2,DS</td>
<td>AE2,CE2,DE</td>
</tr>
<tr>
<td>COMP00(All Comp)</td>
<td>AS,BS</td>
<td>AE,BE</td>
<td>AS</td>
<td>AE</td>
</tr>
<tr>
<td>COMP01</td>
<td>AS1,BS1,DS</td>
<td>AE1,BE1,DE</td>
<td>AS1</td>
<td>AE1</td>
</tr>
<tr>
<td>COMP02</td>
<td>AS2,BS2,FS</td>
<td>AE2,BE2,FE</td>
<td>AS2</td>
<td>AE2</td>
</tr>
</tbody>
</table>