Securing Information in 4.0: Setting up the Gatekeepers

Maria Silva, Business Intelligence Manager
Dunn Solutions Group
Who am I?

Maria Silva – Business Intelligence Project Manager

Work at Dunn Solutions Group – 13 years

Full-service IT consulting firm

Founded in 1988

Offices
- Chicago
- Minneapolis
- Raleigh
- Bangalore, India
What do we do?

- BI Practice
  - Migrations
  - Data Warehouse Design and Implementation
  - SAP BW & R/3 + Business Objects BI
  - Dashboards
  - Reports
  - Data Quality and Data Integration
  - Predictive Analytics
  - Budgeting, Planning and Consolidation
  - Training

- Application Development Practice
  - Custom Application Development / E-commerce
  - Portal (including SharePoint Services)
  - Mobile Application Development
  - Content Management
Setting the Gate Keepers
Why do we want to secure?
Why do we want to secure?

Regulatory, Market and Social Pressures
Why do we want to secure?

Regulatory, Market and Social Pressures

Information Provision & Effectiveness is a must to be competitive
Why do we want to secure?

Regulatory, Market and Social Pressures

Information Provision & Effectiveness is a must to be competitive

Information Security Initiatives
Bottom Line:

Consistent

Accurate

Secured
Different Gates to Set in our BI deployment

Infrastructure Gates
- Detached Gates
- Configurable Gates

Functional Gates
- User Access
- Function Access
- Folder Access

Data Gates
Different Gates to set in our BI deployment

- **Infrastructure Gates:** Physical and Electronic Access to the Environment

- **Functional Gates:** By function and role that would need to be supported by the tool

- **Data Gates:** Restricting specific data based on our functional gates
INFRASTRUCTURE GATES

Basic Architecture

Legend
- SAP BI platform
- SAP BI clients and data sources

Central Management Console (CMC)
- BI Launch Pad
- Rich Clients / Web Clients
  - Crystal Reports
  - Dashboard Design
  - Web Intelligence
  - Analysis Explorer

Semantic Layer
- Universe
- Business Views

Semantic Layer Tools
- Information Design Tool
- Universe Design Tool

Connections
- Connections
- ODA Connections

Web Server
- Central Management Server

Input File Repository Servers
Output File Repository Servers
Lifecyle Management Database
Adaptive Job Servers
Adaptive Process Servers

Reporting Data Warehouse
Enterprise Information Management
- Data Services
- Data Steward

Non SAP Systems
- Alternate ERP, CRM and other solutions

Other DMP Solutions
- SAP Products, Lifecycle Support

Data Sources
Securing the Infrastructure Gates (Detached)

- Guidelines for Disaster:
  - FRS (Objects stored with Company Proprietary Data)
  - CMS Database
  - Database Information Keyfile (.dbinfo Key file)
Securing the Infrastructure Gates (Detached)

- Guidelines for Disaster:
  - FRS (Objects stored with Company Proprietary Data)
  - CMS Database
  - Database Information Keyfile (.dbinfo Key file)

\"Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\"
Securing the Infrastructure Gates (Detached)

- Guidelines for Disaster:
  - FRS (Objects stored with Company Proprietary Data)
  - CMS Database
  - Database Information Keyfile (.dbinfo Key file)

Add additional encryption to FRS through third party software (server and/or laptops)
Guidelines for Disaster-Continuation:

- **Environment Protection:**
  - Web Browser to Web Server: Use SSL protocol for your network communication between servers and clients
  - Web Server to BI Platform: Firewalls are commonly used for this. Communication between BI platform components
Securing the Infrastructure Gates – Configurable

- Strictly enforce corporate password changes policies
  - Enforce mix case
  - Must Contain at Least N Characters

- Restrict Multiple Logons:
  - Internal mechanism that enforces a time delay (0.5-1.0 second) between logon attempts.
  - Customizable options that you can use to reduce the risk of dictionary attacks.
Ticket Mechanism

Server

Session Variable

Client

Active Trust Relationship

SSL

Cookie

Logon Token Information
Securing the Infrastructure Gates – Configurable 2

- Active Trust Relationship: BI Platform components can process users request and actions without prompting credentials
  - Logon Tokens: Contain User Session Information
    - Number of Minutes
    - Number of Logons

- User Guest Account Restrictions

- Access to CMS must be restricted to local access only
Data processing security modes:

- Default Data Security Processing Mode
- FIPS (Federal Information Processing Standard FIPS 140.2)
  - It is not backward compatible with legacy BI platform client tools or applications.
  - Data processing standards and guidelines prohibit the use of hard-coded encryption keys.
  - Required to secure sensitive data according to FIPS 140-2 regulations.
FUNCTIONAL GATES
Functional Gates

- Functional Gates relate to Authentication and Authorization
  - Authentication
    - Is this a valid user?
    - Can the user log in to the application?
  - Authorization
    - What part of the application or data can a user access?
The security model of a BI application is concerned with three distinct areas:

- **User Authentication** – Controls access to the application
- **Functional access** - what the users can do
- **Folder access** - what folders and objects can a user see.
User Access

- Authentication methods available in SAP BO 4

<table>
<thead>
<tr>
<th>Enterprise</th>
<th>AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>SAP</td>
</tr>
<tr>
<td>Oracle EBS</td>
<td>Siebel</td>
</tr>
<tr>
<td>JD Edwards</td>
<td>Peoplesoft</td>
</tr>
</tbody>
</table>

SAP BusinessObjects

Windows

LDAP

Oracle E-Business Suite

Siebel

JD Edwards

PeopleSoft
Functional and Folder Access

- Define Functional User Groups
  - To define roles
  - To define Application access

- Define Data User Groups to grant access to folders
  - To define folders access
  - To define what connections / Universes can be used
I. Don’t skip it, you need a conceptual security model.

II. Ideally your group structure and folder structure align with your administration security structure
   ▪ Create individual administrator accounts for each administrator in the system and add them to the Administrators group to improve accountability for system changes.

III. Use Access Levels when possible (View, Schedule, View on Demand, Full Control, No Access)

IV. Differentiate the View and View on Demand. They make a big difference!

V. Set rights and access levels on top-level folders – Let inheritance work!

VI. Set rights always at the folder level
VII. Set up an audit policy and periodically review your deployment

- Permissions Explorer
- Check Relationships
- Security Query

VII. Document your security matrix

VIII. Keep it as simple as possible

IX. Review the rights of Everyone group members and assign security accordingly.
Data Gates

DB or 3rd Party Security

Data Security Profiles

Security Tables

Third party security

Business Security Profiles
Universe Profiles

- A security profile is a group of security settings that apply to a universe published in the repository.
  
  - **Data Security Profiles** have security settings defined on objects in the data foundation and on data connections. (only for relational universes)
  
  - **Business Security Profiles** have security settings defined on objects in the business layer.
Data Security Profiles

- Connection
- Query Controls
- SQL Generation Controls
- Row Access
- Alternative Table Access
Data Security Profiles - Connection

- Only Secured Connections
- The replacement Connection must be of the same type as original
- Relational Connection Types:
  - SAP NetWeaver BW relational databases
  - SAS relational databases
  - Other relational databases
- Multisource can be replaced for each connection
Data Security Profiles – Control Settings

- Replace default query limits set in BL

<table>
<thead>
<tr>
<th>Query Limit</th>
<th>Possible values</th>
</tr>
</thead>
</table>
| Limit size of result set to  | • True and a numerical size between 0 and 2147483647 rows  
|                              | • False                                                                        |
| Limit execution time to      | • True and a numerical size between 0 and 2147483647 minutes  
|                              | • False                                                                        |
| Warn if cost estimate exceeds| • True and a numerical size between 0 and 10000 minutes  
|                              | • False                                                                        |
Data Security Profiles – SQL Generation Controls

SQL Generation Controls

- Defines replacement query options set in BL and DF properties

<table>
<thead>
<tr>
<th>Query Option</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow use of subqueries</td>
<td>True, False</td>
</tr>
<tr>
<td>Allow use of union, intersect and minus operators</td>
<td>True, False</td>
</tr>
<tr>
<td>Allow complex operands in Query Panel</td>
<td>True, False</td>
</tr>
<tr>
<td>Multiple SQL statements for each context</td>
<td>True, False</td>
</tr>
<tr>
<td>Multiple SQL statements for each measure</td>
<td>True, False</td>
</tr>
<tr>
<td>Allow Cartesian products</td>
<td>Warn, Prevent</td>
</tr>
</tbody>
</table>
Row Access

- Restricts the rows returned by a query
- A Where clause is added when profile is assigned
- SQL can use: @Variable and @ Prompt
- Multisource Universe could refer to tables in any connection
- Can not include calculated columns or derived tables

A user who has the right to edit SQL can change the Where clause
Data Security Profiles – Alternative Table Access

- To define replacement tables

A user who has the right to edit SQL can change the replacement table
Business Layer Profiles

Create Query
- Define Universe Views
- Business Layer Objects

Display Data
- Grants or denies access to the data retrieved by objects

Filters
- Define Filters using Objects in the BL
Business Layer Profiles

There are two ways to grant or deny objects:

- **By business layer view:** Grants or denies all objects in a view. The All business layer views option allows you to grant or deny all views defined for the universe.
- **By object:** You can grant or deny the objects listed below.

- Dimensions
- Attributes
- Measures
- Calculated members
- Filters
- Prompts
- Named sets
- Folders: Grants or denies all objects in the folder.
- Analysis dimensions: Grants or denies all objects in the dimension.
- Hierarchies: Grants or denies all objects in the hierarchy.
Security Profile Aggregation

- Two main ways to aggregate Security Profiles:
  - Priority – Use the Security Editor to determine priority
  - Restriction Level
    - Very restrictive
    - Moderately restrictive
    - Less restrictive

Review the way restriction levels are applied in each type of security settings. The restriction levels for Connection and SQL may differ, check the IDT documentation.
Security Profiles Facts

- More than one Profiles can be assigned (G or U)
- Profiles are stored independently
- Changes in DF or BL do not affect Security Profiles
- Security Editor to preview net profiles
- Profiles are deleted if a Universe is deleted
A Security Table is a table created expressly to be used in a Universe Designer and allow to restrict the number of rows. This security tables uses @BOUSER Variable in a join to determine what rows a particular uses can see.
SAP Security

- The SAP ECC Security is carried to BW and it is BW/BeX queries the ones that restrict rows based on SAP user. It carries over the SAP authentication to be active in the SAP Business Objects Platform.
You are being watched
Summary

- Security in your BI Environment is not be taken lightly.
- SAP Business Objects offers many ways, Supported or Configurable, to allow us to have a secured environment.
- Make sure to cover all three security areas discussed in this presentation and take note of best practices.
- Take advantage of existing security infrastructures to assist you in securing your BI deployment and data transmission.
- Make sure you know what are the Corporate Security Policies in regards to Data and Data Transmission.
- Create a BI Security Policy Document and have it approved by the CTO or similar role.
Other resources:

- SAP BusinessObjects Business Intelligence 4.0 Business Intelligence Platform Administrator Guide

- SAP BusinessObjects Business Intelligence 4.0 Information Design Tool Guide

- Quick Reference Getting Around Information Design Tool
  (http://scn.sap.com/docs/DOC-22142)

- SAP BusinessObjects Business Intelligence 4.0 Publishing Guide

- Business Objects Security Paper from Pal Alagarsamy
Thank you for participating.

Please provide feedback on this session by completing a short survey via the event mobile application.

SESSION CODE: 0605

Learn more year-round at www.asug.com