Global Information Assurance Certification Paper

DB2 protection under RACF

Marcos Pereira Leite

GIAC Security Essentials Certification (GSEC)

GSEC Pratical Assignment V1.4b Option 1

January, 2004

Table of Contents

Abstract	3
Introduction	3
DB2 Protection	4
RACF	7
RACF Advantages	8
Migration Plan	9
RACF Protection	10
Duties Segregation	12
Summary	13
Bibliography	13
Appendix A – DB2 Privileges	16
Appendix B – DB@ Administrative Authorities	20

Abstract

This assignment is about centralizing protection of DB2 databases in the RACF. This material does not explain in detail how DB2 and RACF works. The principal objective is to show the importance and advantages of the protection of DB2 objects in the RACF database to people who as part of their responsabilities need to implement such protection or, out of curiosity, desire to understand better how it works.

The paper first explains the privileges in the DB2 database and the differences between the privileges and the levels of access control to DB2 objects. The second part shows how the RACF protection works and the advantages of this type of protection over native protection in the case of DB2 objects. At last, this paper shows how to carry out the migration protection, the possible complications that it may entail and how a duty segregation in the DB2 environment might be implemented.

The background required to read this text is a general knowledge of DB2 and RACF. The basic concepts and mechanisms presented here could serve as a basis for further study of these concepts and implementations

Introduction

"Legacy mainframe applications form the foundation of the IT infrastructure at many companies. About 70 percent of the world´s data resides on mainframes and 85 percent of all business transactions are processed on these machines". (1)

Mainframes is an industry term for a large computer, typically manufactured by a large company for mission-critical applications such as global weather forecasting and scientific research and other large-scale computing purposes such as manufacturing, healthcare and commercial applications. Although many people errouneously think the opposite, most of the big companies in the e-business world rely on mainframes to supply the commerce and eletronic infrastructure of their business. Keeping up with security, IBM has enhanced the hardware encryption capabilities in their last versions, adding Kerberos, x509V3 digital certificate, LDAP and VPN+IKE supporting. (18)

OS/390 Security Server is the IBM product that protects resources and controls security in the z/OS and OS390/MVS mainframe environments. Working closely with the operating system's existing features, it provides improved security for all the installation data. The Resource Access Control Facility (RACF) was developed in 1976 to allow companies to secure their organization's information. (2) In March 1996, the RACF application was integrated into the OS/390 Security Server product, which encompasses a wide array of security components, designed to provide enterprise security. The RACF provides user authentication,

flexible access control to resources, auditing and exits for installation or written routines.

The Release 4 Security Server from September 2002, supports DB2 Version 7, Enhanced PKI Services and other features (17), but since the RACF Release 4 and DB2 version 5, the access to the DB2 objects can be controlled through RACF.

RACF protection of DB2 resources allows administration and audit from a single point of control, validates a user ID before permitting it access to a DB2 object and controls access with security rules.

DB2 is the IBM relational database management system that operates as a formal subsystem of the operational system (20, p 7-12) and is setting the standard for quality, reliability and high avaibility. It supports documents, images, audio, video, and spatial data.

Although encryption garantees that unauthorized users don´t access data, it is a very costly approach because encryption affects performance and limits the data sharing accross applications. Whenever it is possible and doesn´t expose sensitive data, the least cost solution is a hybrid solution with encryption, duties segregation, centralized accesss control, an active policy control and proper audit procedures.

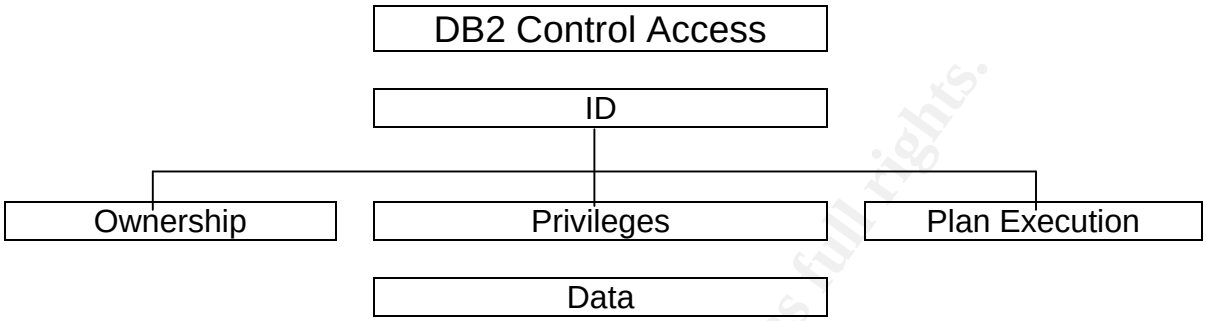
In most companies, database administration and security is done by the database administrators using the database native access control. Teams with business rules knowledge, like the development team, should not access production data. End-users, who are divided in groups depending on their profiles, are the only ones who should access data in a systemic way.

For that reason companies must segregate their technical teams based on their functions, and, keeping in mind the advantages of DB2 protection under RACF, should move DB2 control access from native DB2 catalog to RACF database, leaving DBA users with only physical access, not logical access.

DB2 protection

Privileges are permissions granted to users to perform some action on database objects (See Appendix A). These object privileges include SELECT, INSERT, UPDATE, DELETE on tables and EXECUTE on plans. For instance, if you have a SELECT privilege on a table, this means you can SELECT or read the table. Object privileges are granted on an object-by-object basis. There are two types of privileges within DB2. Object privileges, which can be Explicit or Implicit, and other grouped privileges owned by the administrative authorities. When a user receives an administrative authority, he also receives a set of privileges according to this authority. The privileges and authorities together control the database management, utility operations and access to the database objects.

Implicit privilege is associated with the ownership of one object. When a user creates an object, he implicitly gains some privileges on it that cannot be revoked. To change ownership, you must drop and re-create the object with a new owner. Explicit privilege is obtained as a result of a GRANT command. By granting the privilege to execute an application plan or package, you can eliminate the need to grant other privileges on tables separately.



>Three ways within DB2 to access its data (20)

The most important administrative authority is the Installation SYSADM. When the DB2 is installed, it is possible to select two user identifiers to be named Installation SYSADM and Installation SYSOPR. These identifiers are not stored in the DB2 catalog. They are important when the catalog is not available and DB2 cannot check authorizations. In such situations, only one installation SYSADM authority can start the DB2. They have the SYSADM or SYSOPR privileges, which are not checked against RACF protection, are not audited and can only be changed by substituting the file that contains the subsystem initialization parameters.

Next is the System Administrator, SYSADM. It is the highest administrative authority in a DB2 subsystem. Among his/her privileges, he/she can access all data, create or drop any DB2 object and GRANT or REVOKE any privileges to users or groups. The System Control, SYSCTRL, is a System Administrator without access to the data unless explicitly obtained through an authorization, who has the responsibility of administering a system containing sensitive data. The System Operator, SYSOPR, has privileges to issue most DB2 commands, terminate utilities and carry out other activities associated with the operation of the subsystem. The highest authority at the database level is the Database Administrator, DBADM, who has all privileges in a specific database. Other administrative authorities are the PACKADM, which has all package and collections privileges, the DBMAINT, who has privileges to run certain utilities and responds to database maintenance and the DBCTRL, who is a DBMAINT for a specific database. (3, p 112) (See Appendix B) Few people should have these authorities in the production environment.

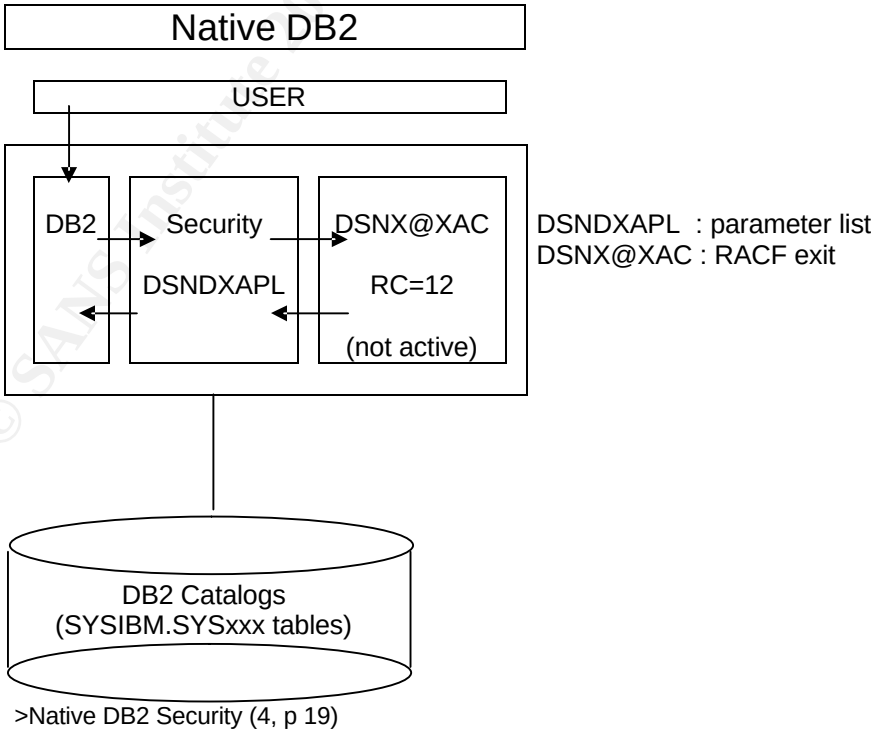
Many privileges and actions are granted to these administrative authorities and the only control over such actions is to audit them. (3, p 113) Audit trace

records attempts to access data, attempts to change tables, and attempts to grant or revoke authority. (20, p 7-15)

In DB2, we have the following objects:

- Tables and views, which are the principal access authorizations points
- Indexes, related to tables, their accesses and performance problems
- Triggers, related to events like insertions and updates in the tables
- Plans and Packages, related to application structures. Plan is the group of SQL commands from a routine and package is the collection of accesses generated by the optimizer and the authorization model. It contains the information needed by DB2 to access data in the most efficient way
- Collections, Stored Procedures, User-Defined Functions and Distinct Types related to development procedures
- Databases and Subsystems related to a group of tables
- Storage Groups, Bufferpools and Table Spaces related to physical structures

It is possible to control the access to DB2 objects by granting or revoking explicit privileges and administrative authorities. An explicit privilege has a specific function as SELECT or INSERT and is given as a result of a GRANT command. By creating a view and granting privileges on it, it is possible to permit access only to specific data. For example, it is possible to give authorization to read (SELECT) solely the sales results from the 2003 year by creating a specific view. Note that if an user has received a privilege, he will keep it until revoked by the same grantor.



>Native DB2 Security (4, p 19)

There are two levels of access control to DB2 objects. Firstly, users must be authenticated in RACF before they can access DB2. This is one of the most basic concepts in database security. Secondly, a user must be authorized in the DB2 subsystem to access its data. These authorizations are kept in the DB2 catalog and are based on users identifiers and groups. They say what and how you can access DB2 data.

There are two different user identifiers. The first serves to identify a user to RACF. It is often the identification used to log on for the session. The second user identifier is the RACF groups to which the user is connected. The user can change his identifier to any of his group identifiers, to execute SQL commands. An explicit privilege can be given to any individual user or group. When a privilege must be available to all users, it is explicitly given to the reserved word PUBLIC.

When native DB2 authorization is used, all the privileges are kept in the DB2 catalog formed by tables and owned by SYSIBM. This catalog contains a record of the privileges related to each authorization name. For example, to create a new table, the DB2 looks in the catalog tables for the proper authorization, comparing the recorded privileges with the name of the authenticated user and the groups to which the user belongs. When you migrate the DB2 security access control to the RACF database, all these privileges must be transported to a RACF profile, relating each object to its privileges, users or group of users.

RACF

RACF provides security to an organization's information environment. The decision to install RACF is not, by itself, enough to ensure adequate security. To be successful, a security implementation always requires a management that is involved with questions of security policy and procedures. (12) Besides utilities and programs, RACF is a database of profiles describing each protected resource in the environment, the access type permitted, and its group of users. Therefore, this database contains the users and their passwords, gathered together in groups, which are then given access to resources. RACF can be set to force many of the current "best-practices" regarding password security (19), such as time elapsed between password changes, password history and password syntax rules. RACF provides discrete, generic and grouped profiles. Discrete profiles have a one-for-one relationship with the resource and should be used for sensitive data (12). The generic profiles are used to protect in only one profile many resources with something in common. To protect resources from the same class which have nothing in common it is used the grouped profile.

The existence of generic profiles greately improved the ease of RACF administration. To implement generic profiles, asterisks are used to represent one or more qualifiers or characters. Percent signs can be used to represent just one character.

There are six levels of access in a RACF profile that may be assigned to a group or user: alter, update, control, read, execute and none. In the RACF protection of DB2 objects are used only the *read* level indicating that the user or group has the privilege specified in the profile or *none* denying this privilege.

RACF advantages

The biggest advantages of RACF security protection for DB2 objects over DB2 native protection are that cascading revocations are eliminated when the grantee looses his privileges and the protection of objects and the creation of their access rules are allowed before the objects are created. Another advantage is the reduction of the required number of profiles. Using patterns you can join several DB2 privileges in one RACF profile, reducing the work required to create and maintain your access control policy. Only those working as DB2 database administrators know how much work is needed to protect each table and view in the DB2 database. Database administrators should not worry with security, but with monitoring, optimizing performance, testing new features and helping application programmers, installing new versions and tuning in their applications.

RACF advantages over native DB2 access control
• Reduces the number of authorization rules that are required to implement your installation security policy, thus reducing administrative complexity and the work required to create and maintain your access control policy
• Provides a more flexible access control mechanism
• Eliminates cascading revocations
• Allows access rules to be defined before a DB2 object is created
• Allows access rules to be preserved when a DB2 object is dropped
• Allows RACF groups to be used for access control, eliminating one of the common reasons for a secondary auth ID exit
• Consolidates security administration and audit for multiple DB2 subsystems or data sharing groups
• Consolidates security administration within the security administration
• Consolidates DB2 audit data with RACF audit data
• Allows access control to be made the responsability of the external security manager, without having to make modifications to DB2 code

>RACF and DB2 Teamed for Security (5, p 1)

Depending on how big the legacy existing applications are, and their privileges, it is not an easy task to migrate the access control from native DB2 to RACF. You must change application privileges, one by one, using RACF facilities, like groups and patterns, grouping together a set of DB2 privileges in one RACF generic profile without compromising the production environment and following your security and environmental priorities.

Migration Plan

As long as most of the installations leave the DB2 security under DBA administration, the first step should be to move the DB2 protection in the production environment to the security team beggining their acquaintance with DB2 privileges and objects.

The migration plan should start with the development environment. The homologation and production environments should be migrated only when the security team is well trained and everything thoroughly tested.

Every enterprise installation has legacy applications, confidential data, complex systems with multiple tables and views, different application roles and systems with interrelations with others. This diversity must be considered in the migration plan. There is no ready strategy.

Possibly the best strategy is to start with the creation of the RACF profiles to substitute the administrative authorities. It is recommended that these profiles should be defined before the RACF exit is activated (4, p 21). Then, you should worry with grouping users with the same privileges into groups defined in RACF. Each of these groups will have a specific profile associated to given actions in the DB2 tables. It will be easier to manage group privileges than individual privileges. Besides this, when maintaining the access list of the profiles, always assign access levels to groups as best pratice dictates that users are not placed there. (16)

Next, application by application, start with the implicit privileges, object by object, tables, views, packages, plans etc, ending with the explicit privileges.

When the migration is planned, the following should be considered:

- The security team, administrators and auditors, involved in the migration plan.
- The development team, participating in each application analysis, to well describe each of the business rules hidden behind the various DB2 privileges.
- The development and end-users involved in perfoming the tests and their experience levels.
- The complexity of the applications.
- The migration schedule.
- What hardware, software and tools will be used, as well as lab environments.
- The migration priority levels.
- The management approval.

Regardless of the resources available, if it is planned to develop or deploy new applications using DB2 databases in any of the environments affected by the

migration plan, they should be protected directly in the RACF database, as this would certainly help by shortening the scheduled migration time.

Proper attention should also be given to customized third-party products. If their necessary DB2 privileges do not satisfy the RACF security policy, the supplier must be contacted. Start by getting a copy of the data dictionary for the tables, the technical documentation and a security manual for the product to better evaluate and understand how the inherent security model works. The security policy must always be followed. In addition, the rules must be definitive in stating and encouraging good security practices.

A sample conversion tool called RACFDB2 may assist you to build the RACF profiles. This tool is described in Ready for e-business: OS/390 Security Server Enhancements (2, p 48-50) and is available on an “AS-IS” basis. This utility converts the contents of the SYSIBM.SYSxxx tables to equivalent RACF profiles.

Because it does not group profiles, the utility output is formed of one RACF profile definition plus one RACF PERMIT command for each necessary user privilege. Once you have the utility output you must evaluate the possibility of combining profiles into grouping profiles to ease implementation and administration. If the DB2 subsystem or application being migrated do not follow standards, the work will be harder, because it will not be possible to group privileges in one RACF profile.

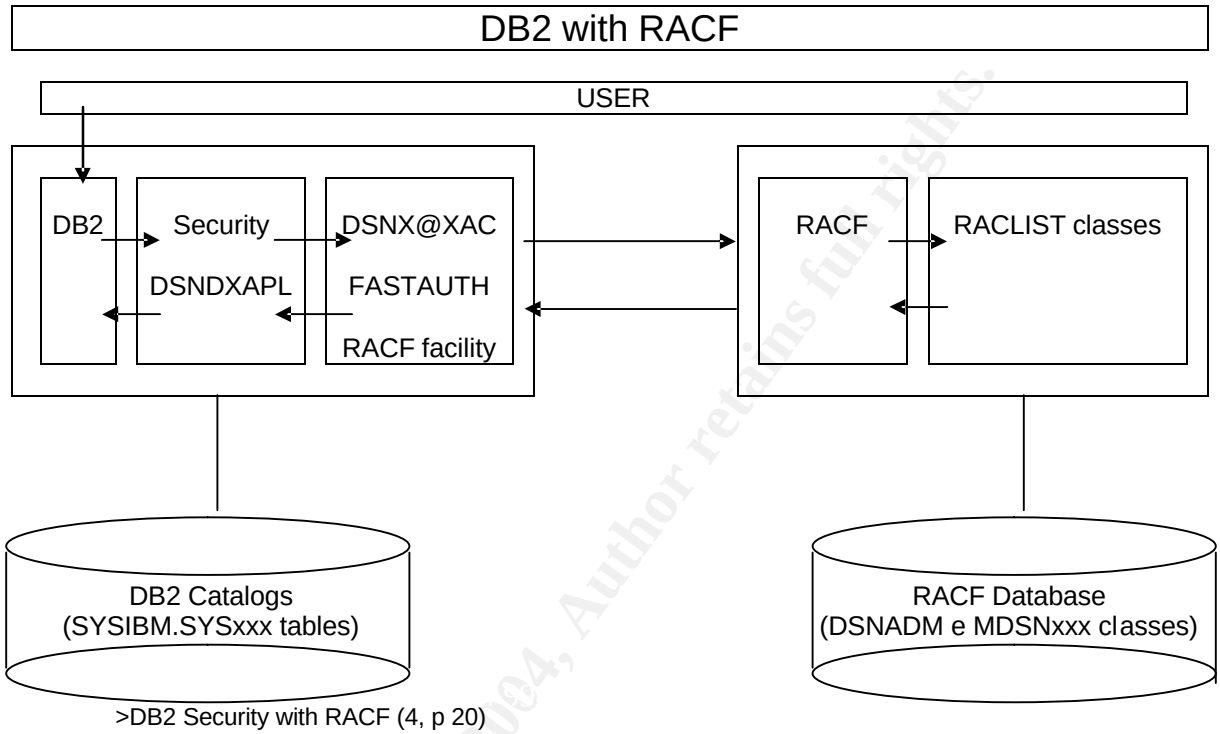
Resuming, the utility must be executed, the approppriate group of profiles selected, refined and grouped using patterns. Run the output script and test the implemented profiles. Then, select another application or group of profiles and restart the migration. Try to use each of these group of profiles as a model to be applied to others applications. In the development environment, for instance, the group of programmers and analysts of each application should share the same group of privileges in their DB2 databases.

Native DB2 to RACF access control Migration Plan
1. Activate RACF classes for DB2 control access interface
2. Activate the DB2 exit
3. Run the utility
4. Select the approppriate group of profiles
5. Refine and group the profiles using patterns
6. Run the script
7. Test the implemented profiles
8. Select another application or group of profiles

RACF protection

The migration plan can be done step-by-step because when the RACF exit is activated, the RACF protection works as a front-end authorization shell. First, the

needed authorization is looked in the RACF databases. If it is found, the access will be granted or negated. If it is not found, then the native DB2 catalog will be verified. This way, it is possible to choose between protecting in the RACF some of the DB2 objects, some of the DB2 subsystems, some of the applications, and any other combination of these protections. This should be used only as part of the migration strategy.



>DB2 Security with RACF (4, p 20)

It is important to understand that the access control can be authorised based on an explicit privilege or on administrative authorities depending on the objects and operations involved. Remember that, for example, if you want to do a SELECT, you must be the owner of the object, have the SELECT privilege, the DBADM or SYSADM administrative authority to do so. First, all possible privileges for an access autorization are searched in the RACF database and if none found, they are all checked again in the DB2 catalog.

This characteristic of the DB2 database control access is very important when a decision is made on what administrative authority each technical group in the enterprise must have to accomplish its functions with the minimum privilege needed.

The DB2 protection in the RACF is accomplished with a different profile rule for each DB2 object type. For instance, when protecting for UPDATE all tables prefixed by *XYZ* from the *APP* application in the DB2 subsystem *SUBS*, what will be created is the *SUBS.APP.XYZ*.UPDATE* RACF profile in the MDSNTB class of the RACF database.

DB2 Object Type	RACF class name	RACF profile
Bufferpool	MDSNBP	subsystem.buffer-pool-name.privilege
Collection	MDSNCL	subsystem.collection-id.privilege
Database	MDSNDB	subsystem.database-name.privilege
Package	MDSNPK	subsystem.collection-id.package-id.privilege
Plan	MDSNPN	subsystem.plan-name.privilege
Storage Group	MDSNSG	subsystem.storagegroup-name.privilege
System	MDSNSM	subsystem.privilege
Table, view, trigger	MDSNTB	subsystem.owner.table-name.privilege
Columns	MDSNTB	subsystem.owner.table.column-name.privilege
Tablespace	MDSNTS	subsystem.database.tablespace-name.privilege
User Defined Type	MDSNUT	subsystem.schema-name.type-name.privilege
User Defined Function	MDSNUF	subsystem.schema-name.function-name.privilege
Stored Procedure	MDSNSP	subsystem.schema-name.procedure-name.privilege
Schema	MDSNSC	subsystem.schema-name.object-name.privilege
JAR	MDSNJR	subsystem.schema-name.jar-name.privilege
Adm Authorities	DSNADM	subsystem.privilege
System Authorities	DSNADM	subsystem.database-name.privilege

>RACF/DB2 External Security Module – Authorization Checking (4, p 58-70)

Duties segregation

Security : implements the installation access plan that says *who* can access, *what* can be accessed and the *intention* (why) of the access. Administers users and groups, connects users to groups, prevents unauthorized access to data and monitors user access of data through auditing techniques. The security team must have SPECIAL attributes in the RACF database to maintain the security policies. This is the most powerful attribute in the RACF database. It gives the user system-wide access and the ability to create, alter and delete profiles. (19) Their actions must be constantly audited.

Auditing : says if the access control is working, what as accessed, by whom and when the accesses were made and checks unauthorized access attempts. It also controls the activities of the security team with reports and logging features, relating all the access requests and policy changes to the solutions adopted by the SPECIAL users. Asks for justifications of unauthorized accesses attempts and if they are acceptable, asks the security team to adjust the roles accordingly.

DB2 Support : tests and implements new features and versions. When it is necessary to migrate the production environment to new versions, it must have SYSADM administrative authority and be audited. Databases with very sensitive data, must be encrypted, so nobody except end users can access the data.

Production DBA : monitors and manages database structure and space allocation. They must have SYSCTRL administrative authority. This way they do not have access to data and do have the necessary privileges on all tables, plans, packages and collections to change their structures, start, stop, repair, recover, trace and monitor the DB2 subsystems,

Development DBA : manages performance problems. They can have specific access to DB2 catalog tables to understand the production environment, explain access methods and index usage. They should discriminate production changes and ask Production DBA for their implementations.

Production, Operators : manages applications versions, migrations from the development to the production environments, synchronization, timetable and the results of the batch jobs, starts and stops the tasks.

End-Users : access the databases through online transactions and file browsing.

Installation SYSADM and SYSOPR : their passwords are kept in a safe. They are only used when requested by the DB2 SUPPORT to the SECURITY and properly justified and documented (so it can be later audited).

Other administrative authorities like DBCTRL, DBMAINT and DBADM can be given to a group of users with technical responsabilities for a time period to execute specific tasks.

Summary

In most companies, database administration and security is done by the DBA using the database native access control. Sometimes in these companies, the security mechanism used is to give everyone full access to everything in the database, trusting that everyone will use the data as intended.

It is important that no one makes assumptions regarding what users will be doing in the database. Data, in a systemic way, can be accessed only by end users. For that reason, companies must segregate their technical teams based on their functions. Moreover, considering all the advantages of DB2 protection under RACF, this is a key reason for moving DB2 control access from native DB2 catalog to RACF database, leaving DBA users with physical access, but not logical access.

Bibliography

1. Mattsson U., Protegrity, Protecting DB2 Data
   http://www.quest-pipelines.com/newsletter-v4/0403_A.htm

2. Ready for e-business: OS/390 Security Server Enhancements, IBM Redbook
   http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg245158.html

3. DB2 UDB for OS/390 and z/OS V7 Administration Guide, -
   http://publibz.boulder.ibm.com/epubs/pdf/dsnagh13.pdf

4. Nelson M., RACF and DB2 Teamed for Security, IBM Corporation, June 02

http://www.share.org/proceedings/sh95/data/S1733.PDF

5. Nelson M.,Jordan M, Miller R., RACF and DB2 Teamed for Security, Technical Support, June 98
http://www.naspa.com/PDF/98/06-pdf/T9806001.pdf

6. DB2 for MVS DRDA Server: Security Considerations GG24-2500-00
IBM International Technical Support Organization, April 95
http://www.frc.utn.edu.ar/campus/ibm/abstract/gg242500.htm

7. DB2 Product Family, IBM Corporation
http://www-306.ibm.com/software/data/db2/

8. Schumacher R., Easing Development Migration to DB2 UDB, Embarcadero Technologies
http://www.embarcadero.com/resources/tech_papers/easingmigration.pdf

9. Miller R., DB2 for z/OS & OS/390 Security, Oct, 2001 - http://www-1.ibm.com/servers/eserver/zseries/zos/racf/pdf/DB2_Security_Overview_2001_10_27.pdf

10. Zikopoulos P., The Database Security Blanket, Mar, 2001 - http://www-106.ibm.com/developerworks/db2/library/techarticle/zikopoulos/0102_zikopoulos.html

11. DB2 Administration Guide
http://webdocs.caspur.it/ibm/web/udb-6.1/db2d0/db2d0.htm#ToC

12. OS/390 V2R10.0 SecureWay Security Server RACF Security Administrator´s Guide – Controlling Access to DB2 Objects, IBM Corporation
http://www-1.ibm.com/servers/eserver/zseries/zos/racf/library.html

13. IBM DB2 Migration Tollkit, IBM Corporation
http://www-306.ibm.com/software/data/db2/migration/mtk/

14. DB2 UDB e-business Guide, IBM Corporation
http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246539.html

15. RACF DB2 Migration Tool, IBM Corporation,
http://www-1.ibm.com/servers/eserver/zseries/zos/racf/racfdb2.html

16. Sharber B., Protecting MVS Data Sets with RACF, 2003, Sans Institute

17. RACF History, IBM Corporation,
http://www-1.ibm.com/servers/eserver/zseries/zos/racf/racfhist.html

18. Armstrong I., Mainframe Security, Feb 2003, SC Magazine, http://www.scmagazine.com/scmagazine/2002_02/feature.html

19. Denton J.R., An Introduction to Security Features in Security Server (RACF), 2002, Sans Institute

20. MVS Planning Security, IBM Corporation http://publibz.boulder.ibm.com/epubs/pdf/IEA5F400.pdf

Appendix A – DB2 privileges

Implicit Privileges of ownership	
Object Type	Privilege
Storage group	To alter or drop the group and to name it in the USING clause of a CREATE INDEX or CREATE TABLESPACE statement
Database	DBCTRL or DBADM authority over the database, depending on the privilege (CREATEDBC or CREATEDBA) that is used to create it. DBCTRL authority does *not* include the privilege to access data in tables in the database.
Table space	To alter or drop the table space and to name it in the IN clause of a CREATE TABLE statement
Table	To alter or drop the table or any indexes on it
	To lock the table, comment on it, or label it
	To create an index or view for the table
	To select or update any row or column
	To insert or delete any row
	To use the LOAD utility for the table
	To define referential constraints on any table or set of columns
	To create a trigger on the table
Index	To alter, comment on, or drop the index
View	To drop, comment on, or label the view, or to select any row or column
	To update any row or column, insert or delete any row (if the view is not read-only)
Synonym	To use or drop the synonym
Package	To bind, rebind, free, copy, execute, or drop the package
Plan	To bind, rebind, free, or execute the plan
Alias	To drop the alias
Distinct type	To use or drop a distinct type
User-defined functions	To execute, alter, drop, start, stop, or display a user-defined function
Stored procedure	To execute, alter, drop, start, stop, or display a stored procedure
JAR (Java class for a routine)	To replace, use, or drop the JAR

>Table DB2 privileges – DB2 for OS/390 V7 Administration Guide (3, p 118)

Explicit Privileges		
Object Type	Privilege	Description
TABLE or VIEW	ALTER	to change the table definition
	DELETE	to delete rows
	INDEX	to create an index on the table
	INSERT	to insert rows
	REFERENCES	to add or remove a referential constraint referring to the named table or to a list of columns in the table
	SELECT	to retrieve data from the table
	TRIGGER	to define a trigger on a table
	UPDATE	to update all columns or a specific list of columns
PLAN	BIND	to bind or free the plan
	EXECUTE	to use the plan when running the application
PACKAGE	BIND	to bind or free the package
	COPY	to copy a package
	EXECUTE	Inclusion of the package in the PKLIST option of BIND PLAN
COLLECTION	CREATEIN	Naming the collection in the BIND PACKAGE Subcommand
DATABASE	CREATETAB	to create tables in the database
	CREATETS	to create tablespaces in the database
	DISPLAYDB	to display the database status
	DROP	to drop or alter the database
	IMAGCOPY	to prepare for, make, and merge copies of table spaces in the database and to remove records of copies
	LOAD	to load tables in the database
	RECOVERDB	to recover objects in the database and report their recovery
	REORG	to reorganize objects in the database
	REPAIR	to generate diagnostic information about, and repair data in, objects in the database
	STARTDB	to start the database
	STATS	to gather statistics and check indexes and referential constraints for objects in the database
	STOPDB	to stop the database

System Privileges	
ARCHIVE	to archive the current active log, to give information about input archive logs, to modify the checkpoint frequency specified during installation, and to control allocation and deallocation of tape units for archive processing
BINDADD	to create new plans and packages
BINDAGENT	to bind, rebind, or free a plan or package, or copy a package, on behalf of the grantor. The BINDAGENT privilege is intended for separation of function, not for added security. A bind agent with the EXECUTE privilege might be able to gain all the authority of the grantor of BINDAGENT.
BSDS	to recover the bootstrap data set

Subsystem Privileges	
CREATEALIAS	to create an alias for a table or view name
CREATEDBA	to create a database and have DBADM authority over it
CREATEDBC	to create a database and have DBCTRL authority over it
CREATEESG	to create a storage group
CREATETMTAB	to define a created temporary table
DISPLAY	to display system information
MONITOR1	Receive trace data that is not potentially sensitive
MONITOR2	Receive all trace data
RECOVER	to recover threads
STOPALL	to stop DB2
STOSPACE	to obtain data about space usage
TRACE	to control tracing

Use Privileges	
USE OF BUFFERPOOL	to use a buffer pool
USE OF STOGROUP	to use a storage group
USE OF TABLESPACE	to use a table space

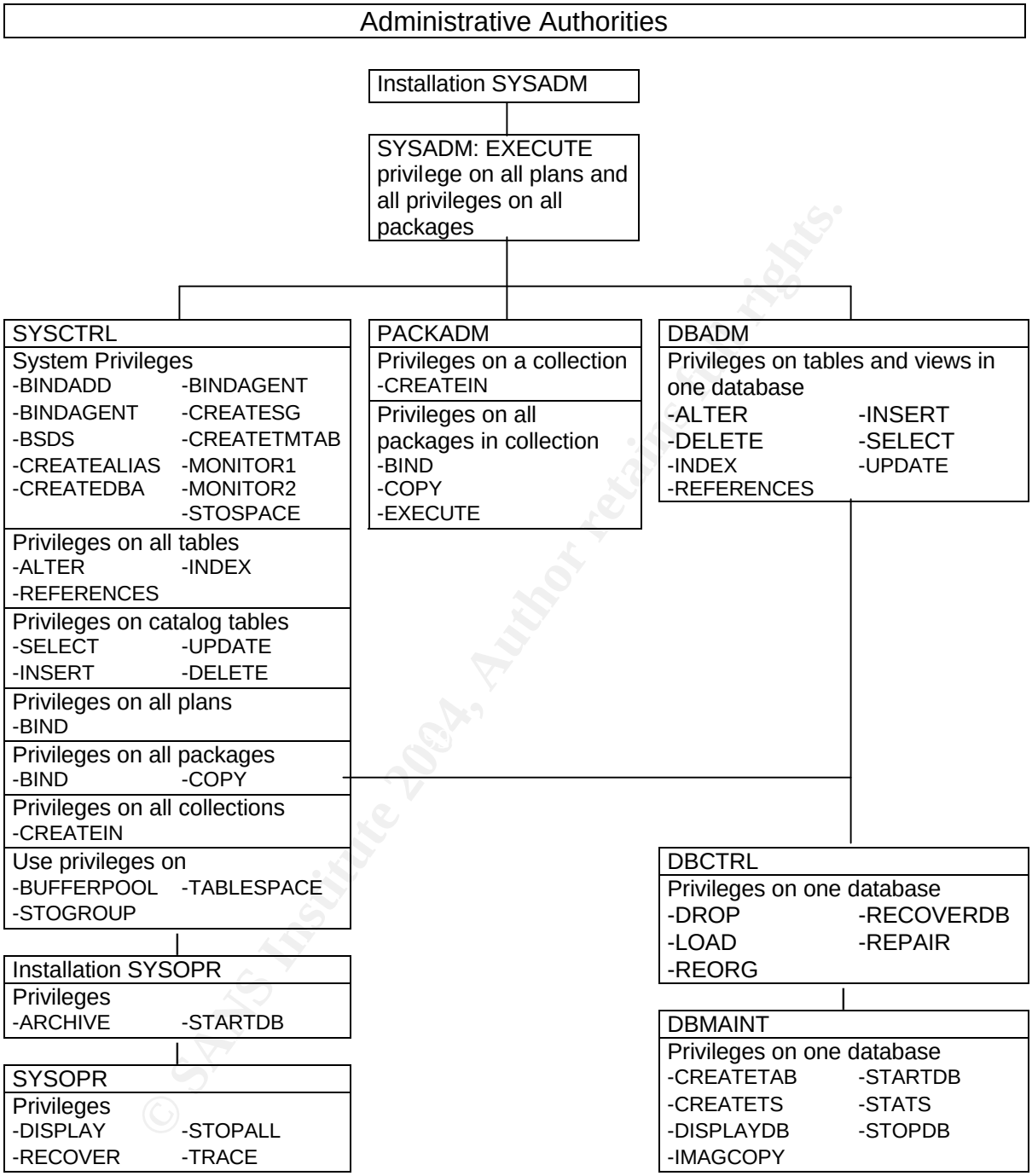
Schema Privileges	
CREATEIN	to create distinct types, user-defined functions, triggers, and stored procedures in the designated schemas
ALTERIN	to alter user-defined functions or stored procedures, or specify a comment for distinct types, user-defined functions
DROPIN	to drop distinct types, user-defined functions, triggers, and stored procedures in the designated schemas

Distinct Type and Java class privileges	
USAGE ON DISTINCT TYPE	to allow use of a distinct type
USAGE ON JAR	to allow use of Java class

Routine Privileges	
EXECUTE ON FUNCTION	to allow use of a user-defined function
EXECUTE ON PROCEDURE	to allow use of a stored procedure

>Table DB2 privileges – DB2 for OS/390 V7 Administration Guide (3, p 107-110)

Appendix B – DB2 Administrative Authorities



Each authority includes the privileges in its box plus all the privileges of all authorities beneath it
Installation SYSOPR can do things that SYSADM and SYSCTRL cannot

>Table DB2 authorities – DB2 for OS/390 V7 Administration Guide – Chapter 10 (3, p 111)