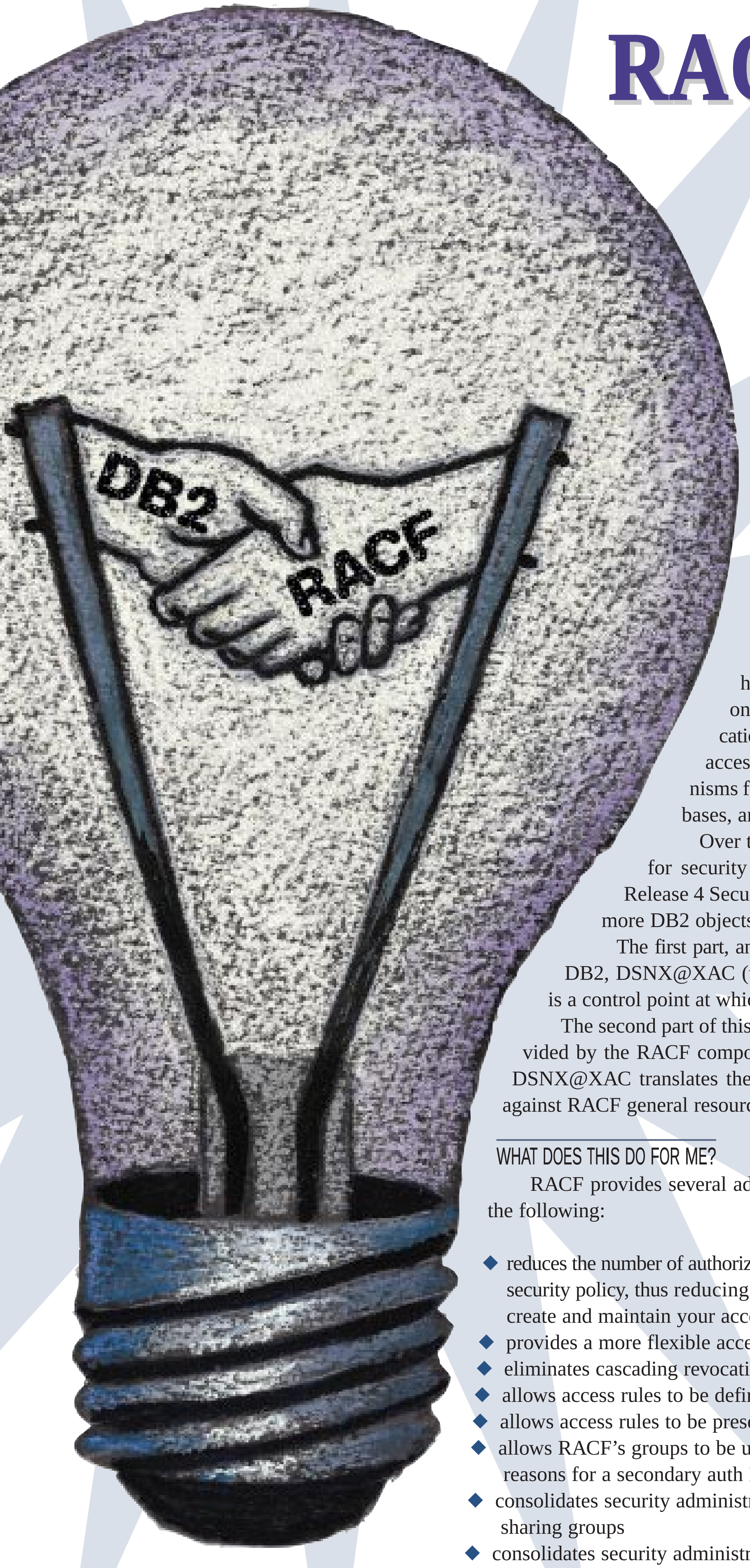
RACF AND DB2: FOR SECU

BY MARK NELSON, MICHAEL JORDAN AND



The combined power of the RACF component of OS/390 Release 4 Security Server and DB2 Version 5 provides a mechanism to control access to DB2 objects.

SINCE its first release in 1983, IBM's premier large system database product, DB2, has had a split personality for security. DB2 has always relied on the operating system (OS/390 or MVS) for user identification and authentication and when verifying if a user has access to the DB2 subsystem. However, it had its own mechanisms for controlling access to DB2 objects, such as tables, databases, and views.

Over the years, the need for a consolidated control mechanism for security evolved. Now, with the RACF component of OS/390 Release 4 Security Server and DB2 Version 5, access to these, and many more DB2 objects, can be controlled through RACF.

The first part, and the heart of this new support, is a new control point in DB2, DSNX@XAC (the DB2 Access Control Authorization Exit Point). This is a control point at which non-DB2 code is called to perform security functions.

The second part of this support is a new "plug-in," DSNX@XAC, which is provided by the RACF component of the OS/390 Release 4 Security Server. RACF's DSNX@XAC translates the DB2 access control decision into one or more checks against RACF general resource classes.

WHAT DOES THIS DO FOR ME?

RACF provides several advantages over native DB2 for access control, including the following:

- reduces the number of authorization rules that are required to implement your installation's 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's 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 organization

TEAMED
RITY

ROGER MILLER

- consolidates DB2 audit data with RACF audit data
- allows access control to be made the responsibility of the external security manager, without having to make modifications to DB2 code

CHOICES

You have many options in controlling DB2 using RACF. These include which RACF general resource classes are used, which DB2 resources are protected by RACF, and which resources are protected by DB2.

Choosing RACF General Resource Classes

One of the most significant choices is choosing which RACF general resource classes are going to hold your DB2 access profiles. You have two choices:

- place profiles for all DB2 subsystems into one set of RACF general resource classes
- create one set of RACF general resource classes per DB2 subsystem

Placing all profiles into one set of RACF general resource classes offers several advantages:

- you can use IBM-supplied general resource classes, thus eliminating the need for installation defined classes that require an IPL to install
- you can consolidate all of your DB2 access control for all DB2 subsystems into one place
- you can use RACF's GENERICOWNER facility to delegate the administration of DB2 access control at the subsystem, database, tablespace, table or even view level

There are also advantages to using a set of RACF general resource classes for each DB2 system:

- isolation of profiles from differing DB2 subsystems
- fewer profiles in each general resource class

RACF's DSNX@XAC has assemble-time controls that allow you to control what general resource classes are used and how the RACF resource names are generated. These controls are implemented as variables in RACF's DSNX@XAC code. Changing these variables requires you to re-assemble and re-install DSNX@XAC and restart your DB2 subsystem.

> You have many options in controlling DB2 using RACF. These include which RACF general resource classes are used, which DB2 resources are protected by RACF, and which resources are protected by DB2.

Choosing What is Protected by RACF

DB2's DSNX@XAC control point and RACF's plug-in provide you with flexibility in determining whether RACF or DB2 make the access control decision. You make this choice by creating RACF profiles that match the DB2 resource names that you want protected by RACF. Any DB2 resource name that does not match a RACF profile causes RACF's DSNX@XAC to return a return code that tells DB2 to use its traditional access control mechanism (SYSIBM tables).

The table in Figure 1 shows the RACF general resource classes and resource names associated with each type of DB2 object. The general resource names and class names shown assume that you are placing all of your DB2 access controls into one set of general resource classes — a set of classes that are shipped with RACF by IBM.

Checking Multiple Privileges

Every access control decision within DB2 is composed of a series of checks. For example, what authority do you need to SELECT a row from a table? Clearly, the SELECT privilege on the table will suffice. However, if you lacked that privilege, you could have also had DBADM on the database that contained the table or SYSADM on the DB2 subsystem that contained the table.

RACF checks all the privileges and authorities that could give you access just as if the check were being made by DB2. RACF documents these checks in the chapter "RACF/DB2 External Security Module: Authorization Checking" in the *OS/390 Security Server Security Administrator's Guide*.

ADMINISTRATION

With this support, the RACF RDEFINE, RALTER, and RDELETE commands are used to define your installation's access control policy to your DB2 data. You can use RACF's powerful generic profile facility or RACF variables to have a single RACF profile cover many DB2 objects, including objects from multiple DB2 subsystems.

For processing efficiency and speed, these profiles are loaded into MVS data spaces using RACROUTE REQUEST=LIST,GLOBAL=YES and are accessed using the RACROUTE REQUEST=FASTAUTH facility. Each class (and its member class if grouping profiles are used) is loaded into its own MVS data space and is shared among all of the DB2 subsystems that are executing on that MVS image. Profiles in the data space may be refreshed using the RACF SETROPTS RACLIST(class-name) REFRESH command.

MAKING CHANGES TO RACF'S DSNX@XAC

Implementing your choices is a simple matter of modifying the DSNX@XAC that is shipped with RACF. You set these options in the source code to DSNX@XAC, and then assemble, link-edit, and install the code in your DB2 libraries. To make the exit active, you must restart your DB2 subsystem. Check out the *OS/390 Release 4 Security Server* (RACF) *System Programmer's Guide* for complete details on how to install the RACF/DB2 External Security Module.

DIFFERENCES, LIMITATIONS, AND OTHER THINGS THAT YOU SHOULD KNOW

There are some instances in which the DSNX@XAC exit cannot pass sufficient information to RACF to make an access control decision. These are IMS applications

Figure 1: The RACF General Resource Classes and Resource Names Associated With Each Type of DB2 Object

DB2 Object	RACF General Resource Class	RACF Resource Name
Tables and views	MDSNTB/GDSNTB	DB2subsystem.owner.table.privilege or DB2subsystem.owner.table.column.privilege
Databases	MDSNDB/GDSNDB	DB2subsystem.database.privilege
Plans	MDSNPN/GDSNPN	DB2subsystem.plan.privilege
Packages	MDSNPK/GDSNPK	DB2subsystem.collection.plan.privilege
Bufferpools	MDSNBP/GDSNBP	DB2subsystem.bufferpool.privilege
Collections	MDSNCL/GDSNCL	DB2subsystem.collection.privilege
Table Spaces	MDSNTS/GDSNTS	DB2subsystem.database.tablespace.privilege
Storage Groups	MDSNSG/GDSNSG	DB2subsystem.storagegroup.privilege
System Privileges	DSNADM	DB2subsystem.privilege
Administrative Privileges	DSNADM	DB2subsystem.privilege
Other Privileges	DSNADM	DB2subsystem.privilege

that invoke DB2 and DB2's "-" commands. For these cases, RACF returns the decision to DB2, which then uses its existing control mechanisms. Also, DSNX@XAC is not invoked for either the install SYSADM or install SYSOPR user IDs.

CICS5 must be configured to enable the passing of user identity to the DSNX@XAC exit.

WANT MORE INFORMATION?

For more information about controlling DB2 objects with RACF, see the *OS/390 Release 4 Security Server (RACF) Security Administrator's Guide* (SC28-1915). Information on installing RACF's DSNX@XAC exit can be found in the *OS/390 Release 4 Security Server (RACF) System Programmer's Guide* (SC28-1913) and in the *DB2 Administration Guide* (SC26-8957). Information on RACF and CICS security can be found in the *CICS System Definition Guide* (SC33-1682 for Transaction Server, SC33-1164 for Version 4, and SC33-0664 for Version 3), *CICS-RACF Security Guide* (SC33-1701 for Transaction Server, SC33-1185 for Version 4, and SC33-0749 for Version 3) and the *CICS Resource Definition Guide* (SC33-1684 for Transaction Server and SC33-1166 for Version 4).

SUMMARY

Using this new feature of RACF and DB2 allows you to reap the benefits of industry-leading secure access to data for your business. The combined power of DB2 and RACF await you!

Mark Nelson, advisory programmer, has had a varied 18-year technical and management career in information systems, the last 16 of which have been with IBM. Mark's RACF experience focuses on data reporting and analysis, designing and implementing both the IRRDBU00 and IRRADU00 utilities. Mark is an active speaker on RACF, having spoken to user groups and IBM field representatives on four continents. Mark can be reached via email at markn@vnet.ibm.com.

Michael Jordan, staff programmer, has worked the first eight years of his IBM career in the RACF Develop-ment team. Michael was a designer and developer for the RACF/DB2 External Security Module, working closely with the DB2 Development team to provide this new support. Other projects Michael has worked on include RACF support for APPC/MVS, RACF support for the Parallel Sysplex and the RACF Remote Sharing Facility. Currently, he is working as a member of the OS/390 Parallel Sysplex Development team. Michael can be reached at jordanmj@us.ibm.com.

Roger Miller, senior programmer, is a 29-year veteran of the computer industry, the last 19 of which have been with DB2 for OS/390 development, design, and strategy. In addition to his work with DB2 security, Roger is often involved in the field helping customers make the best use of DB2 and is also a frequent speaker on DB2. Roger has worked on most facets of DB2, ranging from overall design issues to SQL, languages, install, security, audit, standards, performance, concurrency and availability. Roger can be reached at millerrl@us.ibm.com.