Global Information Assurance Certification Paper

Name: Bill Sharber
Course: GSEC
Version of GIAC assignment: Security Essentials Courses [Sep 5, 2002].
This is an original submission.

Protecting MVS Data Sets with RACF

Harold Tipton stated part of computer security "specifically is the protection of data in a system against unauthorized disclosure and modification". [1] On an IBM mainframe RACF (Resource Access Control Facility) can be one of the security components used to protect data. RACF has many specialized classes, which are used to create rules for data protection. This paper will explain how the Data Set class is used to provide data protection of files on a mainframe system.

IBM introduced RACF in 1976[2] to provide a security framework on its mainframe computers. Installing RACF on a system provides no security and by default protects nothing.[3] RACF contains programs, utilities and a database of objects that when called by programs and utilities provides answers to security questions posed to it. When a call (question) is made to RACF, the database is searched and the best match for the request is returned. The answer to that call can be yes, no, maybe, or not found. In the case of file access requests (questions), the MVS operating system makes the call to RACF and then determines the action to be taken with the answer to its question. Is the access request to be allowed for the data requested? In RACF, the Data Set class covers files (data sets) on the MVS system. Examples of data sets that may be covered by profiles in the Data Set class are:[7]

- Sequential data sets.
- Partioned data sets.
- VSAM data sets.
- Tape data sets.
- Production data sets.
- Test data sets.
- System catalogs

A data set profile may be discrete, covering only one file, or it may be generic and cover may files. In the earliest releases of RACF all data set profiles were discrete. The introduction of generic data set profiles greatly improved the ease of administration of RACF data set profiles. Since a generic profile may cover one or thousands of data sets, most installations of RACF today use generic profiles exclusively and this paper will focus on generic profiles. When RACF checks the profiles in the data set class, it will first check to see if there is a discrete profile that exactly matches the data set to be opened. If no discrete profile can be found it will then look for the generic profile that provides the best match for the data set. If a matching profile cannot be found, RACF will look at the Protect All system option to determine the answer to the access question. If Protect All is turned on and a match cannot be found for the data set requested, RACF will fail the access request. If protect all is turned off or in warning mode, RACF will allow the data set request to proceed. These are the reasons why the

answer to the access question can be 'maybe' it is allowed or a 'not found' response can be returned.

When a data set profile is matched, there are six ways a userid can be authorized to access the data set. RACF checks a user's access according to this hierarchy. RACF will stop resource access checking when one of these conditions is matched. There are a couple more ways a user will be allowed access to a data set discussed later in the paper. These six ways are the most common for user access.[3]

1. The user's ID is equal to the first qualifier of the data set name. A has complete access to all data sets that begin with his user ID. A user cannot be denied access to their own data sets.

2. The user is a member of a group or his ID is in the standard access list in the data set profile. Each entry in the access list has an access authority that specifies the access the user has to data sets covered by the data set profile. Access authority levels are covered later in the paper. All access levels should be assigned according to the principle of least privilege. No user should have a level of access greater than is necessary to perform his job function.

3. Universal Access Authority (UACC) is the level of access the data owner has decided is acceptable for all users on the system to have. The UACC for a data set profile is normally set to NONE. Since this is the access all users on the system will have, great care should be used when assigning a level of access greater than NONE. Only certain system data sets that all users need to access should have a UACC greater than NONE. Consider the situation where a data set profile covers test data sets and the profile has a UACC of Read. If a user is able get production jobs to reference this profile, he can introduce test data in the production job stream.

4. A user's ID profile is then checked to see if the user has the Operations attribute. The operations attribute is not defined in the data set profile. It is defined in the User ID profile. If a user ID has the system wide operations attribute, the data set access request will be satisfied. The system wide operations attribute should be used carefully and is normally only appropriate for DASD management user IDs.

5. The user is a member of a group or his ID is in the conditional access list in the data set profile. The conditional access list specifies that a user can access the resource when a certain condition is meet. Most often the When Program condition is used in the conditional access list. When program specifies a user can only access the data sets covered by the

profile when executing a specific program. An access level is still used to define the user's access ability.

6. If the user's access request cannot be satisfied by the above methods, warning mode is checked. Warning mode is used when an administrator is creating a new data set profile and is unsure who will be accessing the data sets covered by the profile. If warning mode is set to yes, the request will be allowed to continue and a warning log entry will be created. Warning mode can be a great tool if used properly and the warnings are actively monitored. It does have a couple of drawbacks. While a profile is in warning mode there is essentially no access control on the data sets covered by the profile. All requests for access will be approved. Warning mode can also generate a lot of warning messages to the logs and consoles.

It is important to note that RACF will stop checking a user's access when the access request is satisfied. If the request is satisfied by the access list, the UACC, operations attribute and warning mode are not checked. If a DASD management user ID is in the access list for a profile and does not have sufficient access to grant the request, the request will fail. Be sure not to put any DASD management User ID or group that a DASD management user ID in an access list with less than Alter access. If this happens, the DASD management task will fail.

There are six levels of access that may be assigned to a group or user. These levels of access specify the authority the user has when MVS opens the data set for processing. Access levels can be used in standard access list, specified as the UACC on a profile, or used in the conditional access list. The access levels are hierarchical and are presented below with the highest level first.[4]

1. Alter access is the highest level of access. It allows a user to perform any action on the data sets covered by the profile. Alter access is used when the user needs to allocate, delete, move, rename or scratch the data sets covered by the profile.

2. Update access is used when the user only needs to modify data in an existing data set covered by the profile. Update access does not give the user the ability to create new data sets or delete existing data sets covered by the profile. If a data set covered by the profile is a partioned data set, often called a PDS, the user will be able to create and delete members in the data set. MVS calls RACF for access when a data set is opened. In the case of a PDS, it is not called when member of the data set is opened. Native RACF cannot provide granular access protection to members in a PDS. Access is controlled at the data set level and not at the PDS member level.

3. Control access can be considered a special update. It is used to update in place VSAM files. All the rules of update access apply to control access.

4. Read access gives the user the ability to browse data in a data set or execute a program in a data set.

5. With Execute access a user can run a program in a data set, but cannot browse the data set.

6. If None access is specified, the user has no access to the data set.

As noted earlier if a user with the Operations attribute is in the access list, the user will have that level of access. A user with operations attribute can be limited or denied access by specifying an access level less than ALTER access. If the operations attribute user is in the access list with None access, the user will not have access to the data sets covered by that profile.

Standards for creating data set profiles follow the conventions of data set names on MVS. You cannot create a data set profile that violates the MVS data set naming conventions.

- The profile must begin with an alphabetic or national character.
- A profile name can be one or more qualifiers in length.
- Each qualifier can be up to eight characters in length.
- The first character in a qualifier must be alphabetic, but the remaining characters can be numeric or national characters.
- Each qualifier must be separated by a period.
- Generic profiles end in one or more asterisks. A double asterisk assumes Enhanced Generic naming is turned on.
- An asterisk (*) can represent one or more qualifiers or characters.
- A double asterisk can represent zero or more qualifiers or characters.
- A percent sign (%) is used to represent one character.
- There cannot be an asterisk or a percent sign in the first qualifier.
- A data set profile including periods cannot be longer than 44 characters.

- A double asterisk can only be used once in a data set profile. A profile can contain multiple single asterisks.

Examples of valid data set profile names are below. HIGHLVL refers to the first qualifier of the data set name. It can be any first valid qualifier. Second and third refer to the second and third qualifiers of the name.

- Highlvl.* or Highlvl.** - These profiles will cover data sets beginning with HIGHLVL that are not covered by a more specific data set profile.

- HIGHLVL.S* or HIGHLVL.S** - These profiles will cover any data sets beginning with HIGHLVL.S and will match zero or more characters after the S. They will also cover zero or more qualifiers after the S. They will cover data set names: HIGHLVL.S or HIGHLVL.SECOND or HIGHLVL.SEC.THIRD

- HIGHLVL.SE%.* - These profiles will cover any data set beginning with HIGHLVL.SE and having only one character in the third position of the second qualifier and zero or more following qualifiers. Examples are HIGHLVL.SEC or HIGHLVL.SEC.THIRD

- HIGHLVL.SE*.* - These profiles will cover any data set beginning with HIGHLVL.SE and having zero or more remaining characters in the second qualifier and zero or more subsequent qualifiers. Examples are HIGHLVL.SE or HIGHLVL.SE.THIRD or HIGHLVL.SECO.THIRD or HIGHLVL.SECOND or HGHLVL.SECOND.THIRD

A user can also get access to a data set included in the Global Access Table. Profiles for high use system data sets are place in the Global Access Table. The Global access table works much the same as UACC on a data set profile except the table is checked before the RACF database is queried for a data set access request. It is loaded in to system memory and therefore decreases response time and system resource utilization. The access level assigned to a data set in the table is the access all users will have to the data set. Care should be used in adding profiles to the table and establishing the access level. If a match is made on a profile the table, no further access checking is performed. There are no audit records created for access granted by entries in the Global Access table. The data set class does not contain entries for the Global Access Table. It is in the GLOBAL general resource class and can be displayed with the following command. [3]

TSO RLIST GLOBAL DATASET ALL

Entries to the table are made using the General Resource ISPF panels or by batch statements. Two entries that installations should have are listed below. The first one gives all users access to their own data sets. Remember earlier in the

paper it was stated that all users have complete access to their own data sets and you cannot deny a user access to their own data sets. This entry will improve performance for access that will always be granted.[4] The second entry is an example of identifying a data set that all users will need to access and granting all users access to the resource.

&RACUID.*/ALTER (G)
SYS1.BRODCAST*/UPDATE (G)

Another method of access is only for started tasks. Started tasks are like service accounts in Windows. They perform a specific function. Some system delivered started tasks must run as privileged or trusted. If a started task is privileged or trusted no access checking is performed. The task will always have access to all resources. Only certain IBM delivered started task should run as privileged or trusted. Started tasks are defined in the Started General Resource class. You can find all started tasks that have been defined as privileged or trusted by running the DSMON report, program ICHDSM00.[5]

When maintaining the access list portion of the data set profile, always assign access levels to groups. Best practice dictates that user IDs are not placed in access lists. Define users, put them in groups and only give groups access to resources. RACF uses the concept of List of Groups access checking to determine the level of access that a user has to a data set profile. If a user is in more than one access group, the user has the highest access provided by any group that he is a member. If user JOE is in groups Accounting and Payroll and group Accounting has Read access to a data set profile and group Payroll has Alter access, Joe will have Alter access to the data sets covered by the profile.[8]

Previously it was noted that UACC and the Global Access Table are two methods to give all users a specified level of access to a data set profile. Another way is to use the access list. This will be processed faster than a UACC entry and will also allow audit records to be created. An asterisk in the standard access list allows all users defined to RACF to have the level of access associated with the asterisks entry. For example instead of specifying a group name on the access list an asterisks can be used and a level of access specified. This will cover all users.[8]

Audit logging is defined in the data set profile. Both access failures and access successes or both can be logged. Access can be specified as ALL, NONE, SUCCESS and FAILURES. Access records can be created by level of access. Auditing can be specified for READ, UPDATE, CONTROL, and ALTER. A few examples of specifying auditing in a data set profile are:

- Audit ALL This will create an access record for both successful and unsuccessful access attempts. This should only be used on profiles

covering the most sensitive data. It has the potential to create a large volume of audit records.

- Audit Failures(Read) and Success(Update) This will create an audit record for all unsuccessful attempts to read a data set covered by a profile, but will only create records for successful update and greater accesses.

- Audit Failures(Update) This will only create audit records for unsuccessful Update and Alter access attempts. No audit records will be cut for any successful access. This would probably not be a specification used on a data set profile, but is included here to show the flexibility for specifying audit access controls.

RACF creates SMF type 81 records for audit accesses. The SMF records can be read and a report produced to review access successes and failures. All audit logging can be controlled by user IDs with the system Special attribute or a user ID with the system Audit attribute.

RACF data set profiles can be displayed and administered using ISPF screens delivered by IBM, by or installation customized ISPF screens, third party software, or by TSO command line. This paper will only review examples TSO commands. Once the commands are understood, using the delivered ISPF panels will be easier to understand. .

There are six TSO commands to administer data set profiles. LISTDSDD will display a data set profile. ADDSD will add a data set profile. ALTDSD will change a data set profile. . DELDSD will delete a data set profile. PERMIT will maintain an access list SEARCH will search for existing data set profiles. [9] Below are listed the most common parameters for the commands.

The list data set command is useful for displaying existing data set profiles. LISTDSD DATASET(*data-set-name*...) | ID(*name*...) | PREFIX(*character-string...*) AUTHUSER ALL DSNS

- The DATASET parameter will list one or more data set profiles. To use this parameter the profile name must already be know. Running the SEARCH command prior to the LISTDSD DATASET command is a good way to get the data set profiles to use with the DATASET parameter.

- The first level qualifier of any data set profile must already be defined as a userid or a group. Use the ID parameter to display profiles for one or more know userids or group names.

- Use the PREFIX parameter to display data set profiles beginning with one or more characters. LISTDSD PREFIX(sys1) will list all data set profiles beginning with the character string sys1.

- The AUTHUSER parameter displays the access list and each user or group's access level. To use the AUTHUSER parameter the user must have at least one of the following:
    - The System Special or Auditor attribute.
    - The Group Special or Auditor attribute of the group owning the profile.
    - The high level qualifier of the profile matches the user's ID.
    - The user has at least Alter access in the access list of the profile.
    - The universal access is set to Alter.
- The DSNS parameter is used to display a list of data sets covered by the profile. This is helpful in determining if a profile will cover a data set. Be careful when using this parameter. The generic profile being displayed could cover a large number of data sets.

The ADDSD command is used to add a data set profile. There are several more parameters to the ADDSD command. These are the most used.
ADDSD (*profile-name...*) OWNER(*userid or group-name*) UACC(*access level*) AUDIT(*audit level* | *(access-type*)) DATA(*'installation-defined-data'*) WARNING

- Profile-name specifies one or more profiles to be added. It will be the name of the profile. Refer back to the profile naming conventions listed earlier in the paper for the rules on naming.
- OWNER specifies the userid or the group name that owns the profile. If decentralized management of data set profiles is desired the owner is used in determining who can manage the profile. The owner does not automatically have access to the data sets covered by the profile. Refer back to the ways a user can access a data set covered earlier in the paper.
- Universal access, UACC, has been covered earlier in the paper. It is the level of access that all users will have.
- AUDIT options are listed earlier in the paper.
- Each profile can have up to 255 characters specified by the DATA parameter to describe or document the profile.

- WARNING specifies the data set profile is to be put into warning mode. Warning mode was described earlier in the paper. The default for the ADDDS command is no warning. Only use warning mode when unsure what users will be accessing the data sets covered by the profile.

To use the ADDSD command a user must have the system special attribute, must have the same userid as the first level qualifier, must have at least create authority to a group that matches the profile's first level qualifier or have group special attribute to the group owning the profile.

The ALTDSD command parameters are similar to the ADDDS command parameters. The ALTDS command is used to change an existing data set profile. If a user has the system Audit or group Audit attribute for the group owning the profile, the user can change the Audit options.

The DELDSD command is used to delete existing data set profiles. The syntax of the command is DELDSD (*data set profile name…*). One or more data set profiles can be listed in the command. The rules for that can issue the DELDSD command are the same as the ADDSD command.

The PERMIT command is used to add or remove users or groups from the access list of a data set profile.
PERMIT *profile-name* CLASS(DATASET) ID(*name...*) ACCESS(*access level*) | DELETE WHEN(*program(program-name...*|*)) RESET(STANDARD | WHEN | ALL)

- Profile-name specifies the name of the data set profile whose access list is to be maintained.

- CLASS specifies the class the profile is in. The PERMIT command can also be used to maintain the access list for general recourse profiles. If class is not specified the default is the data set class.

- ID specifies the userids or group names to be added, changed or deleted from the access list. It is common practice to only use group names in an access list.

- ACCESS specifies the access levels the groups or userids listed in the ID parameter are to have. Refer to the discussion of access levels earlier in the paper for an explanation of access levels. The access parameter is not specified when removing a group or userid from the access list.

- The DELETE parameter is only used to remove or delete userid(s) or group(s) from the access list.

- WHEN is used for maintaining the conditional access list. The conditional access list is explained earlier in the paper.
- RESET is used to remove all entries from the standard or conditional access lists.

The SEARCH is a powerful command that has many uses in RACF. This discussion will be limited to the data set class. The SEARCH command can search the data set class for entries that match a character string specified in the mask or filter parameters. The mask or filter parameters are not valid in the same search command.
SEARCH CLASS(DATASET) MASK(*charterstring1, charactersting2*) or NOMASK or FILTER(*filterstring*) USER(*userid*).

- CLASS specifies the class the profile is in. If class is not specified the default is the data set class.

- MASK is used to specify a character sting to match. The first character string is required. The search command will match profiles that begin with the first character string. The second character string is optional. This search command will match profiles that contain the second character string somewhere in the profile name.

- FILTER is much more flexible than mask. It can contain symbolic characters. A % will match any one character in the profile name. A * will match zero or more characters in a profile name. A ** will match zero or more qualifiers in a profile name.

I have provided a brief overview of using the RACF data set class to provide protection for files on a mainframe computer. RACF provides many more features for protecting data on a mainframe. A key element to remember is RACF is rules based. The rules protecting data are not defined with the data as in UNIX or Windows. The rules are defined in RACF.

Bibliography

1. Harold F. Tipton, Handbook of Information Security Management, Access Control Principles and Objectives, Chapter 1-1-1, Types of Information Security Controls. http://www.cccure.org/Documents/HISM/003-006.html

2. IBM web site
http://www-1.ibm.com/servers/eserver/zseries/zos/racf/racfhist.html

3. Vanguard Security, RACF Overview presentation.
http://www.share.org/proceedings/sh96/data/S1731.PDF

4. Mary Beth Delphia, Writing Rules with RACF
http://manena.tamu.edu/bizarre/dsnres.html

5. Stu Henderson, Interpreting Output from the RACF DSMON Utility
http://www.stuhenderson.com/XDSMNTXT.HTM

6. Mitchell H. Levine, Access Requirements For Sensitive Operations Functions Within an MVS Environment
http://www.auditserve.com/articles/art_18.htm

7. RACF Starter System for MVS
http://www-1.ibm.com/servers/eserver/zseries/zos/racf/pdf/racf_starter_set_mvs_gg243120.pdf

8. RACF Security Administrators Guide
http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/ICH1A721/CCONTENTS?SHELF=ICH1K110

9. Arizona State University Web Site
http://www.asu.edu/it/fyi/dst/mainframe/racf/index.html