Global Information Assurance Certification Paper

Basic RACF approach
for z/OS and OS/390 series
GSEC Certification
Practical assignment
Version 1.4c
Option 2

Jean-Michel DESNOUVEAUX
SANS Security Essentials - Track 1 / London
June 2004

Table of contents

Forewarning

Before start my report, i would like to catch your attention to the two following points.

Due to my bad knowledge of english language, I had assistance by one of my neighbor to translate some parts of this report (but not all), so it is possible that some explaination do not show exactly my french translation.

Because i do not have MS Word installed on my computer, but Lotus Word Pro, my report is not arranged exactly like yours; some fonctionalities was not available with this software (notably for Header and Footer part).

Abstract

Usualy manage its security is vital for a company. This company must ensure that only the people correctly identified by it are authorized to enter to make their work. It must be of same for its data processing.

RACF provides a solid security to OS/390 system, but it is not simple to manage, for example it is not always easy to measure the real impact of a field value on the global security.
So the following report must be considered as a basic introduction to RACF.
I wanted to approach simply and succinctly this tool, so I will not go into the technical details, the analysis or further descriptions of the informations.

Just like I will not dwell on the necessity to secure a computer system, all already having been said on the subject

To go in depth about RACF, a lot of documentations and courses are available.

Introduction

To securize accesses to a system, it's necessary to :

- ✓ Identify and verify system users,
- ✓ identify, classify, and protect system resources,
- ✓ Administrate security system (user authorization, resources accesses, ...)
- ✓ List, control and audit accesses and violations

Each user must have only one and unique identifier.
To be as shure as possible that the user entering their identifier is really who they say they are, the user validates their identifier by a personal password.
Each user having the same needs or not, you determine a specific protection for ressources and you class users by authority level .
And naturaly to supervise all this system you log all commands used by whoever.

RACF is one of the products that meets all these specifications and more, as :

- Flexible control of access to protected resources
- Protection of installation-defined resources
- Ability to store information for other products
- Choice of centralized or decentralized control of profiles
- An ISPF panel interface
- Transparency to end users
- Exits for installation-written routines (Allow applications to use the RACF macros)

For all these reasons, RACF is very used in IBM environment mainframe.

RACF Version 1 Release 1 was born in September 1976.
The most recent RACF version is actualy Version 2 release 2.

The Purpose of RACF

Resource Access Control Facility (RACF) is a software security product that protects information by controlling access to it. RACF also controls what you can do on the operating system and protects your resources.
It provides this security by identifying and verifying users, authorizing users to access protected resources, and recording and reporting access attempts.

During authorization checking, RACF checks the resource profile to ensure that the resource can be accessed in the way requested and that you have the proper authorization to access the resource. The necessary user-resource requirements must match before RACF grants the access request to a protected resource.

RACF retains information about the users, resources, and access authorities in **profiles** on the **RACF database** and refers to the profiles when deciding which users should be permitted access to protected system resources.

The RACF's Actors

RACF help to control the Who / What / How of a request.
The Who is the user identifier, the What is for target ressource name, and the How is the envisaged access type.

User could be a person defined as a single data-processing object or as being attached to a group (logical object unit) having a common point such as :

- Member to same service
- Member to same function
- Member to same category

These persons or group of persons are defined with profiles within RACF Databases.
The resource is described by a profile whose name, class and identity informations are also defined within RACF databases.
The access type could be a simple read, a creation/deletion, an update or a submission.

Profiles represent the rules supplied to RACF and which are stored within its databases.
Four types of profiles exist :

① User profile
② Group profile
③ Dataset profile
④ General Ressource profile

All these profiles will allow you to determine the capacity of each user in term of access, distribution of authorizations and control.

The access power, or operationnal, result in granting of **OPERATION** privilege.

The distribution of the authorizations power will allow the managing of profiles and will be granted by the **SPECIAL** privilege

Finally the supervisor power will allow the follow-up of conformity the rules of the Opérationnal power and distribution of the authorizations. It will be affected by the **AUDITOR** privilege.

The User

The user is a person requesting a service to a computer system through a job, a started task, from TSO or a CICS transaction, IMS, DB2, etc...
He is identified by a userid stored in a record (Profile), within a RACF file, containing :

- an identifier,
- the user name,
- their password,
- their privileges,
- their default group of membership,
- the groups to which they are attached and their privileges in these groups,
- the owner of identifier,
- some additional segments.

We can categorize the different users as follows:

- **Security Administrator**: The security administrator has the overall responsibility for RACF implementation.
- **Group Administrator** : During planning, the group administrators are user representatives who represent major application areas.
- **Other Administrators** : Others users who administre the relationship produtcs
- **Auditor** : The auditor provides guidance on good auditing practices related to data security and user access. The auditor determines and selects the necessary RACF logging and reporting options to provide an effective of security measures.
- **Technical Support** : The system programmer who provides technical support for RACF installs RACF in the system and maintains the RACF database.
- **Operator** : The user with the OPERATIONS attribute has authority to perform certain "housekeeping" operations on RACF-protected resources (for example, dump/restore).
- **End User** : The end user is the person who is using the RACF-protected system.
  The end user logs onto the system and accesses the resources on the system.

The Group

The RACF user must always work in a group. So, the authorizations are given to the group not to the individual person. That allows :

- ✓ to simplify the management of the authorizations
- ✓ to define a user unit having the same needs

The group is identified by a GROUPID stored within a record (Profile), of an RACF file, and containing :

- The identifier of group,
- the owner of this group,
- the group name to which he is himself attached (higher group),
- the groups names being attached to him (sub-groups)
- the access authorization through a terminal
- an additional segment

The Resources

A resource can be anything from the moment that we can name it in RACF.
It could be files, volumes of bands, terminals, transactions, programs, commands, etc...
It will be defined in RACF by :

- the class name,
- the name of the object or collection of objects that it contains,
- the owner name,
- the implicit acess authorizations with a universal access (UACC) (for the users nondefined in RACF) or explicit (for the users defined in RACF),
- the standard or conditional access list.

These ressources will be protected by one of the following profiles :

- **Discrete profile** : Discrete profiles have a one-for-one relationship with a resource-one profile for each resource. Discrete profiles provide very specific levels of control and be used for sensitive resources.
  A discrete profile can protect a single resource that has unique security requirements.
  A discrete profile matches the name of the resource it protects and cannot exist independently of the resource.

- **Generic profile** : Generic profiles have a one-for-many relationship.
  One profile controls access to one or more resources whose names contain or character strings that RACF uses to associate them with each other.
  A generic profile can protect several resources that have a similar naming structure and security requirements. Specify generic characters in the profile name if you want to protect more than one resource with the same security requirements.

- **Grouped profile**: Another type of RACF profile is the grouped profile.
  There may be no way to associate the resources with a common access list based on patterns in the resource names.

Particular case of definition files

To protect a data set, RACF builds a data set profile and stores it in the RACF database.
You can protect tape data sets and the following types of DASD data sets:

* Cataloged and uncataloged non-VSAM data sets
* VSAM data sets
* Data sets that have the same name but reside on different volumes
* Generation data group (GDG) data sets
* Data sets and catalogs with single-level names obtained through an installation-supplied prefix

RACF can also protect data sets that are password-protected.

When generic profile checking is active, RACF protects new data sets automatically if the data set name matches an existing generic profile name.

When you define a resource class, RACF places control information for the new resource class into a class descriptor table. The control information includes:

- ✓ The resource class name
- ✓ The syntax rules for the resource names within the class
- ✓ The location of the auditing and statistics flags for the class

Administering Security

The security administrator's job can range from helping high-level management initially define corporate security policy to authorizing individual end users to access RACF-protected resources.
As security administrator, you are responsible for implementing RACF at your installation. You have the authority to review and approve all implementation phases, select the resources to be protected, and plan the order in which protection is implemented. You are the authority for all RACF implementation questions. You decide the degree to which decentralization of security controls takes place.

You create profiles for the implementation team, select the team members, and direct their efforts.

Although you have responsibility for overall security at your installation, you can decentralize much of the security operation by delegating various RACF security responsibilities to assistants. You can appoint:

- ✶ Group Administrators
- ✶ Technical Support
- ✶ Auditor

In certain installations, it is possible that some of these functions might be combined.

To make this administration, RACF has specific commands
The RACF commands include operands with which you specify the various user attributes, group authorities, and access authorities. RACF places the information it receives from the commands into various profiles (user, group, data set, and general resource profiles), which it keeps in the RACF database and uses to control subsequent access to resources.

RACF Command list

ADDGROUP (AG)	Define a new group to RACF
ADDSD (AD)	Add RACF protection to data sets with either discrete or generic profiles
ADDUSER (AU)	Define a new user to RACF and establish the user's relationship to an existing RACF-defined group
ALTDSD (ALD)	Modifiy an existing discrete or generic data set profile or add, modify, or remove RACF protection for a single volume of a multivolume, non-VSAM DASD data set
ALTGROUP (ALG)	Change information in a group profile
ALTUSER (ALU)	Change the information in a user's profile, including the user's system-wide attributes and access authorities
CONNECT (CO)	Connect a user to a group, modify a user's connection to a group, or assign the group-related user attributes
DELDSD (DD)	Remove RACF protection from tape or DASD data sets that are protected by either discrete or generic profiles
DELGROUP (DG)	Delete a group and its relationship to its superior group from RACF
DELUSER (DU)	Delete a user from RACF. This command removes the user's profile and all user-to-group connections for the user
DISPLAY	Use the DISPLAY command to display a listing of entries in the signed_on_from list maintained by RACF
HELP (H)	Obtain information about the function, syntax, and operands of RACF commands that are documented in the RACF Command Language Reference
LISTDSD (LD)	List information included in tape and DASD data set profiles
LISTGRP (LG)	List details of specific RACF group profiles
LISTUSER (LU)	List the details of specific RACF user profiles.
PASSWORD (PW)	Change your password, reset a user's password, or change the paswword interval.
PERMIT (PE)	Maintain the lists of user and groups authorized to access a particular resource. RACF provides two types of access lists : standard and conditional
RACLINK	Use the RACLINK command to administer (define, approve, delete or list) RRSF User ID associations
RALTER (RALT)	Alter RACF profiles for ressources belonging to classes specified in the class descriptor table, change the global access checking table, change the list of security categories and levels.
RDEFINE (RDEF)	Define to RACF all profiles belonging to classes specified in the class descriptor table, create entries in the global access checking table and in the lists of security categories and security levels, and define classes as profiles in the RACGLIST class for which RACF will save RACLISTed results on the RACF database
RDELETE (RDEL)	Delete RACF profiles belonging to classes specified in the class descriptor table
REMOVE (RE)	Remove a user from a group and assign a new owner to any group data set profiles the user owns on behalf on that group
RESTART	To restart an RRSF function in the RACF subsystem address space
RLIST (RL)	Display information on ressources belonging to classes specified in the class descriptor table

RVARY	Activate or deactivate RACF, switch primary or backup RACF database, deactivate protection for profiles belonging to classes while RACF is inactive, select mode of operation when RACF is enabled for sysplex communication
SEARCH (SR)	Obtain a list of RACF profiles, users an groups.
SET	Use the SET command to set the operational characteristics for RRSF at your installation
SETROPTS (SETR)	Set system-wide RACF options dinamically
SIGNOFF	Use the SIGNOFF command to sign off sessions by removing them from the signed_on_from list maintained by RACF
STOP	To shut down the RACF subsystem address space in an orderly manner wit losing any remote RRSF requests
TARGET	Use the TARGET command to define the local and remote nodes for RRSF

As an alternative to using RACF commands to perform administration tasks, you can use RACF's ISPF panels.
If you use the panels, you don't need to memorize command or operand names; you only need to complete the appropriate information on the proper panels.

RACF System Macros

You can tailor RACF using various installation exits to bypass security checking or perform additional security processing or checking.

This part contains the external RACF system macros that other callers can use to invoke RACF or another security product.

The RACF system macros are received as part of the MVS program product; installations receive these macros even if they do not intend to install RACF. The RACROUTE macro instruction is the interface for all products that provide resource control.

The RACROUTE macro invokes the system authorization facility (SAF) router. If RACF is present, the SAF router directs control to the RACF router. If RACF is active, the RACF router then invokes RACF.

High Level Assembler or Assembler H is required to assemble the RACROUTE macros.

The following lists the RACF macros that you can invoke with the full function RACROUTE interface.
IBM recommends that installations use the full function RACROUTE interface instead of the independent RACF system macros. Keywords and macro invocations introduced after Release 1.8.2 are supported only if you invoke them using this RACROUTE interface.

- "***RACROUTE REQUEST=AUDIT:*** *General-Purpose Security-Audit Request*"
  is used to audit requests to use a function or access a resource without authorization checking.
- "***RACROUTE REQUEST=AUTH****: Check RACF Authorization*"
  is used to provide authorization checking when a user requests to use a function or access a resource.
- "***RACROUTE REQUEST=DEFINE****: Define, Modify, Rename, or Delete a Resource for RACF"*
  is used to define, modify, or delete resource profiles for RACF.

- "***RACROUTE REQUEST=DIRAUTH:*** *Check RACF-Directed Authorization to a Sent Message*"
  is used to perform security label authorization checking on messages for installations using SECLABELs.
- "***RACROUTE REQUEST=EXTRACT****: Replace or Retrieve Fields*"
  is used to retrieve or update specified resource profile fields or to encode data.
- "***RACROUTE REQUEST=FASTAUTH****: Verify Access to Resources*"
  is used to provide authorization checking when a user requests access to a RACF-protected resource similar to RACROUTE REQUEST=AUTH. However, RACROUTE REQUEST=FASTAUTH verifies access to resources that have RACF profiles brought into main storage by the REQUEST=LIST macro service.
- "***RACROUTE REQUEST=LIST****: Build In-Storage Profiles*"
  is used to retrieve general resource profiles and build an in-storage list for faster authorization checking. The list is attached to the ACEE.
- "***RACROUTE REQUEST=SIGNON****: Manage PV Signed_On Lists*"
  is used to allow RACF to manage the signed-on lists associated with persistent verification.
- "***RACROUTE REQUEST=STAT****: Determine RACF Status*"
  is used to determine if RACF or another security product is active and, optionally, to determine whether protection is in effect for a given resource class. REQUEST=STAT can also be used to determine if a resource class name is defined.
- "***RACROUTE REQUEST****=TOKENBLD: Build a UTOKEN*"
  is used to modify an existing token.
- "***RACROUTE REQUEST****=TOKENMAP: Access Token Fields*"
  is used to convert a user token (UTOKEN) or a resource token (RTOKEN) into either internal or external format.
- "***RACROUTE REQUEST****=TOKENXTR: Extract UTOKENS*"
  is used to extract a UTOKEN from the current task or address space ACEE.
- "***RACROUTE REQUEST=****VERIFY: Identify and Verify a RACF-Defined User*"
  is used to provide user identification and verification.
- "***RACROUTE REQUEST****=VERIFYX: Verify User and Return a UTOKEN*"
  is used to create a user token (UTOKEN) for a unit of work.
  It provides for propagation of USERID, GROUPID, and SECLABEL for locally submitted jobs and is similar to VERIFY in some respects.

RACF Tools

RACF provides several utility programs that can help you and the RACF system programmer manage the RACF database and extract information from it:

IRRUT100	It's a cross-reference utility program. ➢ If you have the AUDITOR or SPECIAL attribute, you can use the RACF cross-reference utility to find and list occurrences of a user ID or group name in the RACF database. ➢ If you have the group-AUDITOR or group-SPECIAL attribute, you can use these utilities only for a user ID or group that is within your scope of authority. ➢ You can also process your profile or profiles that you own.
IRRDBU00	It's a database unload utility program. You can also use the RACF database unload utility to provide flexibility in analyzing RACF profile information. The output from this utility is a sequential file that is a relational representation of a restructured RACF database.
IRRADU00	It's a SMF data unload utility program. The RACF SMF data unload utility is the IBM-recommended utility for processing RACF audit records. With it, you can create a sequential file from the security relevant audit data.
IRRRID00	It's RACF remove ID utility program. It can help you keep your RACF database current. You can use this utility to remove all references to group IDs and user IDs that no longer exist in or are about to be removed from the RACF database.
IRRMIN00	RACF database initialization utility
IRRUT400	RACF database split/merge/extend utility
IRRUT200	RACF database verification utility
BLKUPD	RACF block update utility
.....	.....

RACF Databases

The RACF database holds all RACF access-control information. RACF processing uses the information from the database:

→ Each time a RACF-defined user enters a system
→ Each time a user wants to access a RACF-protected resource

You maintain your RACF database through commands, macros, and utilities.

The database name table (ICHRDSNT) is a customer-provided load module that describes the RACF databases to RACF.
This table contains entries describing each RACF database and its backup database.
RACF allows you to provide a backup database to which you can switch without a re-IPL should your primary RACF database fail. A backup RACF database reflects the contents of the primary database.
Once the installation has created the backup database, RACF can maintain it automatically.
You can decide to back up all your primary databases, or some of them, depending on the needs of your installation.
Use the RACF database name table (ICHRDSNT) to control the amount of updating to the backup database.

RACF can have as many as 90 primary databases and 90 associated backup databases.

RACF databases can reside on any DASD device that is supported by the operating system, including devices with an address greater than X'FFF' on MVS Version 5 systems. Each volume containing a RACF database should be permanently resident. If RACF is heavily used and you elect to use a single RACF database, plan to put the database on a device accessed by the channel and control unit least likely to impact system performance.

RACF and the other products

RACF provides a repository for information needed by other products when that information relates to users or resources those products deal with.
For example RACF provides additional support for interaction with:

- IMS/ESA
- OpenEdition MVS
- CICS/ESA
- TSO/E
- DFSMS
- PSF/MVS
- APPC/MVS
- NetView
- Message Queue Manager (MQM/ESA)
- CICSplex System Manager (CPSM)
- LAN File Service/ESA (LFS/ESA)

One aspect of the flexibility of RACF is the ability of the security administrator to delegate responsibility for maintaining this information to other administrators on the system.

Conclusion

The RACF licensed program satisfies the preferences of the end user without compromising any of the concerns raised by security personnel. The RACF approach to data security is to provide an access control mechanism that:

- Offers effective user verification, resource authorization, and logging capabilities
- Supports the concept of user accountability
- Is flexible
- Has little noticeable effect on the majority of end users, and little or no impact on an installation's current operation
- Is easy to install and maintain

To end this report, the two most important of these RACF'rules, that you must kept in mind, are probably the following :

Organization : You can define RACF groups to map the existing organizational structure. RACF provides flexibility of control and administration, allowing various degrees of central control and delegated control.

Naming Conventions : You can use your own data set naming conventions. RACF provides a table to help you do this easily. Because implementing RACF security is easier when your installation already has a consistent data set naming convention, you can use the installation of RACF as an opportunity to implement consistent naming conventions.

References

Book title	Name	Doc number	Company
RACF Command Language Reference	ICHCL03	SC28-0733-14	IBM
RACF: General Information	ICHGI03	GC28-0722-17	IBM
RACF Version 2 Release 2 Command Language Reference	ICHMCL01	SC23-3731-01	IBM
RACF V2R2 General Information (GIM)	ICHMGI01	GC23-3723-01	IBM
RACF Version 2 Release 2 Macros and Interfaces	ICHMMI01	SC23-3732-01	IBM
RACF Version 2 Release 2 System Programmer's Guide	ICHMSP01	SC23-3725-01	IBM
RACF Version 2 Release 2 General User's Guide	ICHMUG01	SC23-3728-01	IBM
RACF Security Administrator's Guide	ICHSA03	SC28-1340-10	IBM