GC28-0722-9
File No. S370-20

Program Product

Resource Access Control Facility (RACF) General Information Manual

IBM

GC28-0722-9
File No. S370-20

Program Product

Resource Access Control Facility (RACF) General Information Manual

Program Number 5740-XXH

Version 1 Release 7

IBM

Tenth Edition (July, 1985)

This is a major revision of GC28-0722-8. See the Summary of Amendments following the Contents for a summary of the changes made to this manual. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

This edition applies to Version 1 Release 7 of the program product RACF (Program Number 5740-XXH), and to all subsequent releases until otherwise indicated in new editions or Technical Newsletters. The previous edition still applies to RACF Version 1 Release 6 and may now be ordered using the temporary order number GT00-1731. Changes are continually made to the information herein; before using this publication in connection with the operation of IBM systems, consult the latest *IBM System/370 Bibliography,* GC20-0001, for the editions that are applicable and current.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this publication is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead instead.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for readers' comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM Corporation, Information Development, Department D58, Building 921-2, PO Box 390, Poughkeepsie, N.Y. 12602. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Preface

This manual contains overview and planning information for Version 1 Release 7 of the program product RACF (Program Number 5740-XXH). Installation managers and personnel who are responsible for system data security and integrity will find this manual particularly useful. The manual assumes the reader is familiar with MVS or VM. (Throughout this manual, the term MVS means both MVS/370 and MVS/XA.)

RACF is a program product that provides:

- System security
- Resource access control
- Auditability and accountability
- Administrative control

The chapters in this manual are:

- Chapter 1, which discusses present-day needs for data security, provides a basic description of RACF, and identifies key RACF features
- Chapter 2, which describes the major RACF functions, including RACF generalization, RACF-CICS/VS interaction, and RACF-IMS/VS interaction
- Chapter 3, which explains how you use the RACF commands, ISPF panels, exits, options, and tools, to implement and control RACF
- Chapter 4, which provides a high-level introduction to planning for RACF installation
- Chapter 5, which summarizes the changes made to RACF for Version 1 Release 7 and describes the system requirements for RACF

If you are already familiar with RACF, you might want to go directly to Chapter 5 to read about RACF Version 1 Release 7.

This manual has two appendixes and a glossary of RACF terms. The appendixes are:

- Appendix A, which lists all the RACF commands and briefly explains their functions
- Appendix B, which lists the attributes and authorities required to issue the RACF commands and to use the RACF panels

The following publications contain detailed information about RACF:

- *Resource Access Control Facility (RACF) Security Administrator's Guide*, SC28-1340, which explains RACF concepts and describes how to plan for and implement RACF.

- *System Programming Library: Resource Access Control Facility (RACF)*, SC28-1343, which describes how to install, modify, and maintain RACF.

- *Resource Access Control Facility (RACF) Command Language Reference*, SC28-0733, which contains the functions and syntax of all the RACF commands.

  The *RACF General User Command Reference Card*, SX28-0609, contains information extracted from SC28-0733.

- *Resource Access Control Facility (RACF) Messages and Codes*, SC38-1014, which contains the RACF messages, the routing and descriptor codes, the RACF manager return codes, and the RACF-related system completion codes.

- *Resource Access Control Facility (RACF) Auditor's Guide*, SC28-1342, which describes auditing considerations, as well as how to use the RACF report writer and the data security monitor.

- *Resource Access Control Facility (RACF) User's Guide*, SC28-1341, which explains how to perform common end user tasks.

- *Resource Access Control Facility (RACF) Program Logic Manual*, LY28-0730, which describes the internal logic and organization of RACF. Three microfiche cards complement the program logic manual:

  Resource Access Control Facility (RACF) Data Areas, LYB8-0770

  Resource Access Control Facility (RACF) Macro Usage Table, LYB8-0888

  Resource Access Control Facility (RACF) Symbol Usage Table, LYB8-0889

The "RACF" macros that are shipped with MVS are documented in the following publications:

- *OS/VS2 System Programming Library: Supervisor*, GC28-1046

- *OS/VS2 MVS Supervisor Services and Macro Instructions*, GC28-1114

- *MVS/Extended Architecture System Programming Library: System Macros and Facilities Volume 1*, GC28-1150

- *MVS/Extended Architecture System Programming Library: System Macros and Facilities Volume 2*, GC28-1151

- *MVS/Extended Architecture Supervisor Services and Macro Instructions*, GC28-1154

The publication *Resource Access Control Facility (RACF) Installation Reference Manual*, SC28-0734, applies to RACF Version 1 Release 5, and is no longer updated. Applicable information previously in SC28-0734 now appears in SC28-1340, SC28-1342, and SC28-1343.

The following publications contain detailed information about the RACF/VM Support PRPQ (Program Number 5767-002), which allows you to use RACF with VM systems:

- *Introduction to the Resource Access Control Facility/VM Support PRPQ*, GC24-2297, which contains overview and planning information on the use of RACF with a VM system.

- *Resource Access Control Facility/VM Support PRPQ Reference Manual*, SC34-2296, which identifies and explains the differences between the functions of RACF with MVS and VM systems.

- *RACF/VM Support PRPQ General User Command Reference Card*, SX22-0008, which contains the functions and syntax of the RACF commands on a VM system, as well as some examples of using the commands.

The following RACF self-study courses are available from SRA (Science Research Associates Incorporated):

- *RACF for the Security Administrator*, 32187
- *RACF for Technical Support Personnel*, 32188
- *RACF for the Auditor*, 32189

The *Catalog of IBM Education*, G320-1244, contains more information on these self-study courses.

In addition to the RACF publications, see the documentation for the products that you are using with RACF for additional RACF-related information.

After the general availability of RACF Version 1 Release 7, you can use the following temporary order numbers to order publications for RACF Version 1 Release 6.

- *Resource Access Control Facility (RACF) General Information Manual*, GT00-1731

- *Resource Access Control Facility (RACF) Security Administrator's Guide*, ST28-1340

- *System Programming Library: Resource Access Control Facility (RACF)*, ST28-1343

- *Resource Access Control Facility (RACF) Auditor's Guide*, ST28-1342

- *Resource Access Control Facility (RACF) Command Language Reference*, ST00-1732
- *Resource Access Control Facility (RACF) Program Logic Manual*, LT00-1733

In addition to RACF, you should consider other aspects of security at your installation. The following publications contain information on data security and physical security:

- *MVS Security*, GC28-1400
- *The Considerations of Physical Security in a Computer Environment*, G520-2700
- *The Considerations of Data Security in a Computer Environment*, G520-2169
- *Data Security and Data Processing Volume 2, Study Summary*, G320-1371
- *42 Suggestions for Improving Security*, G520-2797
- *Data Security Controls and Procedures -- A Philosophy for DP Installations*, G320-5649
- *Management Memorandum: Security Features of IBM System/370*, G320-5650
- *Data Security Through Cryptography*, GC22-9062

Contents

Figures

Summary of Amendments

Summary of Amendments
for GC28-0722-9
RACF Version 1 Release 7

This manual includes information about RACF Version 1 Release 7.

RACF Version 1 Release 7 offers significant new facilities, such as program control, tape data set protection, erase-on-scratch, security classification of users and data, and other enhancements designed to provide increased security, usability, and auditability.

The highlights of RACF Version 1 Release 7 are:

(In the following list, MVS means both MVS/370 and MVS/XA.)

- Security enhancements
  - Access control to load modules (MVS/XA only)
  - DASD erase-on-scratch support (MVS/XA only)
  - CICS/VS support enhancements (MVS only)
  - Realtime violation notification (MVS only)
  - Data set protect-all option (MVS only)
  - Tape data set protection (MVS/XA only)
  - Tape bypass label (BLP) processing control (MVS/XA only)
- Authorization checking enhancements
  - Program access to data sets (MVS/XA only)
  - Security classification of users and data
  - Data security monitor authorization (MVS/XA only)
  - RVARY command
- Installation control improvements
  - Control of REVOKE/RESUME by date
  - Class descriptor table and RACF router table split
  - User or terminal time/day-of-week control
- Auditability enhancements
  - Data security monitor (MVS only)
  - Logging OPERATIONS authority

- Usability enhancements
  - Virtual storage constraint relief (MVS only)
  - Enhanced support for RACF ISPF panels (MVS only)
  - LISTDSD and RLIST enhancements
  - ADDSD and RDEFINE modeling enhancements
  - RACINIT without statistics generation

Note: Some of these enhancements are operational only with a particular level of another product, such as Data Facility Product Version 2 Release 1.

Chapter 5 contains detailed information on RACF Version 1 Release 7.

This edition also includes minor technical and editorial changes.

Summary of Amendments
for GC28-0722-8
RACF Version 1 Release 6

This publication now includes an expanded description of the data security monitor. Other minor technical and editorial changes have also been included.

Summary of Amendments
for GC28-0722-7
RACF Version 1 Release 6

This publication has been updated to include information about RACF **Version 1 Release 6**.

Technical information added for RACF **Version 1 Release 6** includes:

- RACF authority delegation
  - Group ownership of profiles
  - User attributes at the group level
- Enhanced RACF security capability
  - RACF password encryption via the DES algorithm
  - Generic profile enhancements
  - Refreshing of the in-storage generic profile lists
- Improved installation control
  - Improvements in failsoft protection
  - Started procedures table enhancements
  - Enhancements to the new-password exit
  - Ability to print warning messages during a "grace period"

- Enhanced auditing capability
  - The auditor may use a new system integrity and security status report
  - The auditor may list any attributes
  - Use of the real data set name in reports
  - Report writer sort by resource owner
  - Table-driven data set naming conventions
- RACF commands in ISPF menu format

Editorial changes have been made, including a new introduction (Chapter 1) and information about how to use the RACF panels, commands, options, and tools available to generate RACF reports (Chapter 3). Information about installing RACF (which is in other RACF books) has been deleted, and a program summary has been added (Chapter 5).

Chapter 1: Introduction

RACF is a program product that functions together with the existing system features of MVS/System Product Version 1 Release 3 or later, and MVS/System Product Version 2, to provide improved data security for an installation. (Throughout this manual, MVS means both MVS/370 and MVS/XA.)

RACF also functions with VM/System Product Release 3 or later, with or without the High Performance Option Release 3.2 or later, when used with the RACF/VM Support PRPQ (Program Number 5767-002).

Why Security?

Advances over the past few years in easy-to-use, high level inquiry languages, the use of small computers, and general familiarity with data processing have created a higher level of "computer literacy". Without a corresponding growth in awareness of good data security practices, these advances could result in a higher likelihood of inadvertent (or deliberate) data exposure. (In this context, data exposure means unauthorized access, modification, or destruction of data.) In parallel, there are two additional trends: the continuing need for information to be on some sort of data base that is easily accessible by authorized users, and the increase in critical assets stored on data bases.

As these and other trends continue, and as the number of users and the ease-of-use of data systems increase, the need for data security takes on a new level of importance. An installation can no longer have some security simply because few people know how to access the data. Installations must actively pursue and demonstrate security and use a security mechanism to control any form of access to critical data.

Security Requirements

A security mechanism should:

- Identify users who wish to access the secured system. Ensure that a unique identifier can be associated with each potential user of the system when the user enters the system.
- Verify that the users are who they say they are. When a user enters the system, ensure that a further level of identification, such as a password, verifies that the user has the correct identifier.

- Allow only authorized users to access the protected resources. Provide users with an appropriate level of access authority for each protected resource.
- Allow a convenient way to administer security. Provide the ability to allow the installation to select the kind of security structure and administration that is needed.
- Record accesses to protected resources. Provide another level of accountability so the installation can see who is using what resources. Allow the installation to define the records it requires.
- Document violations, either immediately or as a user-requested periodic report.
- Be usable by those whose data is being protected. A security mechanism has to be easy to define and easy to use in order to help prevent circumventing the mechanism.
- List the key protected resources and indicate the level of protection that exists for each.

How RACF Meets Security Needs

RACF helps meet the needs for security by providing the ability to:

- Identify and verify users
- Authorize users to access the protected resources
- Log and report various attempts of unauthorized access to protected resources
- Administer security to meet an installation's security goals

RACF provides these functions; the installation defines the users and the resources to be protected.

A specific RACF user, called the security administrator, has the responsibility to define users and resources to RACF. (Alternatively, the security administrator can assign other people to do some of this defining.) As well as defining what resources to protect (DASD data sets, minidisks, tape data sets, DASD volumes, tape volumes, terminals, and so on), the security administrator can define and grant the authorities by which users access the protected resources. Thus, the security administrator sets down the guidelines that RACF uses to decide the user-resource interaction within the installation.

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

Note: On a VM system, the RACF data set is called a **RACF data base**.

Identifying and Verifying Users

RACF uses a **userid** to **identify** the person who is trying to gain access to the system and the **password** to then **verify** the authenticity of that identity. RACF uses the concept of only one person knowing a particular userid-password combination to verify user identities and to ensure personal accountability. On an MVS system, RACF allows the use of an operator identification card (OIDCARD) in place of or in addition to the password during terminal processing. By requiring that a person not only knows a password but also furnishes an OIDCARD, an installation has increased assurance that the userid has been entered by the proper user.

Authorizing Users to Access Resources

Having identified and verified the user, RACF then controls interaction between the user and the system resources. RACF must authorize not only which users may access resources, but also in what way the user may access them, such as for reading or for updating.

Logging and Reporting

Having identified and verified the user, and limited access to resources, RACF records the events where attempted user-resource interaction has occurred. An installation can use logging and reporting to alert management not only to anticipated user activities and system events but also to variances from the expected use of the system.

Administering Security

Because the security requirements at every data processing installation differ, RACF allows an installation to meet its own unique security objectives. RACF enables an installation to administer security in a number of ways:

- Flexible control of access to protected resources
- Protection of installation-defined resources
- Choice of centralized or decentralized control of profiles
- Easy-to-use ISPF panels
- Transparency to end users
- Exits for installation-written routines
- Data security monitor (on MVS systems only)

Flexible Control

RACF allows the installation to set its own rules for controlling the access to its resources by defining what is protected at what level, and who can access protected resources. Because of RACF's flexible design, any installation can tailor RACF to interact with its present operating environment. Because the installation establishes the controls -- while RACF merely enforces them -- each installation can also adapt RACF implementation to changes in its security needs.

Protection of Installation-Defined Resources

In addition to the pre-defined resources, such as data sets, minidisks, terminals, and transactions defined to IMS/VS and CICS/VS, RACF permits an MVS installation to protect it's own installation-defined resources. Installation-defined resources provide a great deal of flexibility in defining what resources an installation can protect.

Choice of Centralized or Decentralized Control

RACF, through its ability to delegate responsibilities, allows the installation to assign security responsibilities at a system-wide or group-wide basis, as the installation requires. RACF also allows different users to perform different security tasks, such as auditing and security administration.

ISPF Panels (MVS only)

RACF administration functions have ISPF (Interactive System Productivity Facility) entry panels and associated help panels. These panels make it easy to enter the RACF commands and their options.

Note: To use the RACF ISPF panels, ISPF Version 1 (IBM Program Number 5668-960) or Version 2 (IBM Program Number 5665-319) must be installed. TSO Extensions (TSO/E) Release 2 or later (IBM Program Number 5665-285), or an equivalent, must also be installed.

Transparency to Users

No users of a data processing system want their data read or altered by other individuals except when they specifically intend for this to happen. Unfortunately, users of all types often hesitate to take steps to protect their data. It is not uncommon to see "live" production data used as test data, or to see data deliberately underclassified to avoid having to use the security procedures that the appropriate classification would demand. In many cases, it is easier to ignore security procedures than to use them. Even conscientious users can forget to protect a critical piece of data. The solution to implementing effective security measures is to provide a security system that is transparent to the user.

With RACF, end users do not need to be aware that RACF is protecting their data. By making use of RACF's administrative capabilities, an installation can make the use of RACF transparent to most of its end users.

Exits for Installation-Written Routines

RACF allows an installation to write its own exit routines to deal with unique security needs. These exit routines can be associated with the RACF commands, or they can deal with authorization checking or user passwords.

Data Security Monitor (MVS only)

The RACF data security monitor (DSMON) allows an authorized user to produce reports on the status of the security environment of an MVS system, especially on the resources that RACF controls. The DSMON reports can be used to compare the actual level of security at an installation with the planned level of security.

Examples of information you can obtain from the data security monitor reports are a list of all the users with the SPECIAL, OPERATIONS, and AUDITOR attributes, a list of the RACF installation exit routines, and a list of the programs in the RACF authorized-caller table.

Basic RACF Concepts

RACF can help meet an installation's security needs, because it allows the installation to define **users** who can access protected **resources**, and, concurrently, to relate **how** users can access the protected resources.

Users

RACF allows an installation to define the users who can access the protected resources, records information about the users in the **user profiles**, and maintains this information in the **RACF data set** (along with all other profiles). The user profile includes (but is not limited to):

- The user's name and identifier
- The user's password
- The user's owner
- The user's responsibilities, authorities, or restrictions while defined to the system. These are called the **user attributes**.
- The user's **security classification**. This classification determines the user's ability to access sensitive resources.

Figure 1 illustrates a user profile. Each RACF-defined user has a user profile.

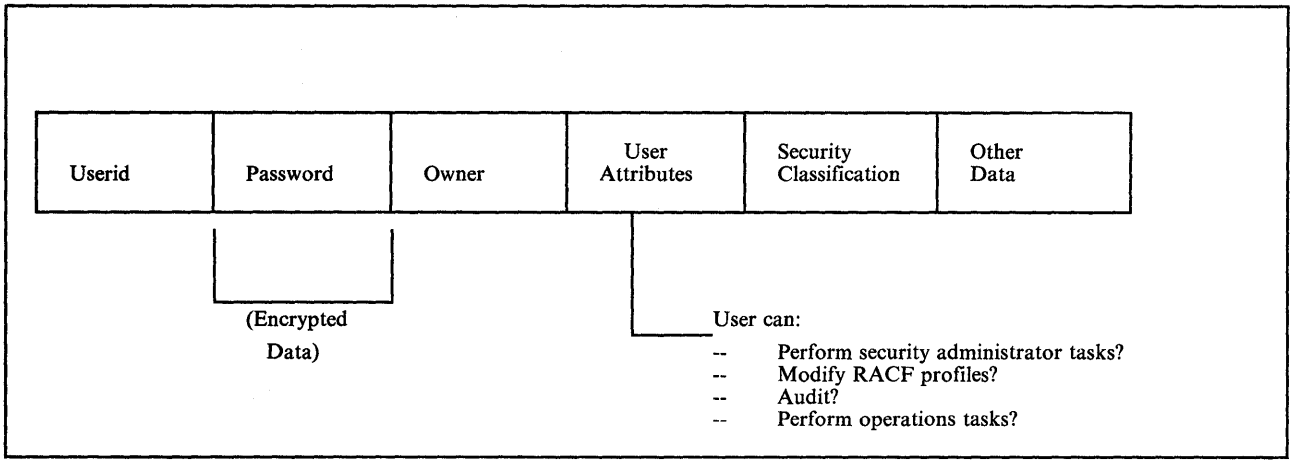

Figure 1. Key Fields in the User Profile

The user attributes define authorities or limits that a specific user has while on the protected system. (Not every user on a protected system has one of the user attributes.) The system-level user attributes include:

- **SPECIAL**, which gives the user full, system-wide control over all the profiles in the RACF data set.
- **AUDITOR**, which gives the user full system-wide responsibility for auditing the security controls and the use of the system resources.
- **OPERATIONS**, which allows the user to perform any maintenance operations -- such as copying, reorganizing, cataloging, and scratching -- on RACF-protected system resources.
- **CLAUTH** (class authorization), which allows the user to define profiles to RACF for classes of pre-defined or installation-defined resources. (A class is a collection of RACF entities with similar characteristics. For example, DASDVOL is the pre-defined class for DASD volumes.)
- **REVOKE**, which prohibits the RACF-defined user from entering the system.

The **security classification** consists of two types of information about the user. The first is the categories that the user belongs to. A **category** is an installation-defined name corresponding to a department or area within an organization with similar security requirements. For example, all of the people who work on the accounting program could be in a category called *accounting*. The second type of information is a security level. A **security level** is an installation-defined name that corresponds to a numerical security level (the higher the number, the higher the security level). For example, a user might have a security level of *confidential*. The installation has defined the security level of *confidential* to be equal to 150.

When a user requests access to a sensitive resource, RACF checks the user's categories and security level to determine whether the user has an adequate "security classification" for that resource.

Groups

With RACF, all defined users belong to at least one group, known as their default group. A group is a collection of RACF users who share common access requirements to protected resources or who have similar attributes within the system. Groups associate similar jobs or projects together for administrative convenience. You can think of the groups as forming a hierarchical or "tree" structure, where each group is "owned" by a superior group. Groups can also "own" resources, as well as users and other groups. Figure 2 illustrates a tree structure of users associated to a group. (Note that subgroups or resources could be associated with groups in a similar tree structure.)

RACF records information about the groups in the **group profile**, which resides in the RACF data set.

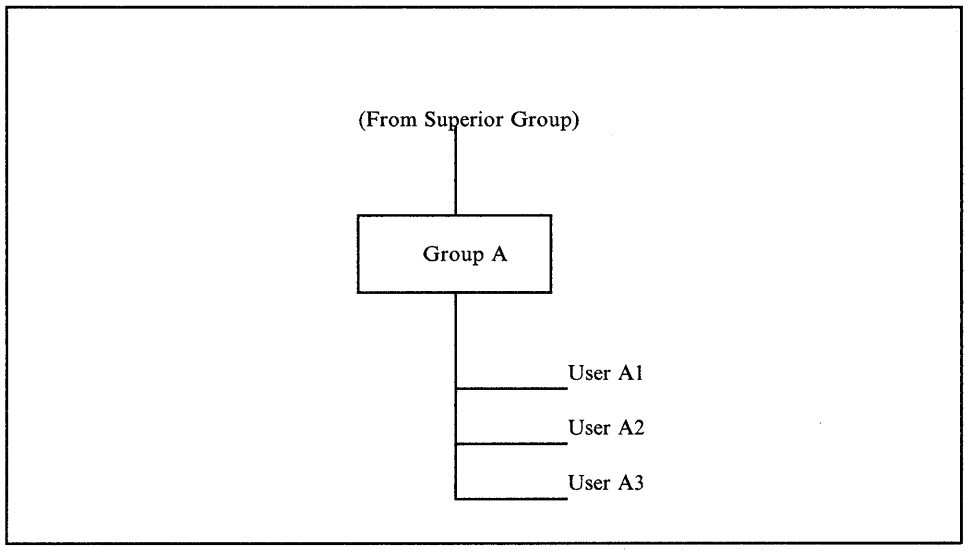

Figure 2. RACF Users Associated with a Group

Connecting Users to Groups

RACF allows users to be members of more than one group. A RACF user who is associated with a group is, in RACF terminology, **connected** to that group.

A group owner -- usually the user who defined the group to RACF -- can define and control the other users connected to the group. The group owner can also delegate various group administrative responsibilities and authorities to various users connected to the group. RACF defines what each user can do when connected to that group in a **connect profile**. The connect profile for a user contains, among other data, the user's **group authorities** and **group-related user attributes**.

The group authorities, which define selected users' responsibilities within the group, are:

- **USE**, which allows the user to access resources to which the group is authorized
- **CREATE**, which allows the user to create RACF profiles for data sets whose name indicates that the data sets are under the administrative control of this group
- **CONNECT**, which allows the user to "connect" other users to the group
- **JOIN**, which allows the user to add new subgroups or users to the group, as well as assign group authorities to the new members

The group-related user attributes are similar to the user attributes at the system level, but they allow the user with the attribute to perform functions pertaining only to the users, groups, and resources associated with the user's group or any of its subgroups. The group-related user attributes are:

- **Group-SPECIAL**, which gives the user full control over the profiles -- user, resource, and group -- within the group
- **Group-AUDITOR**, which gives the user responsibility for auditing the group resources
- **Group-OPERATIONS**, which allows the user to perform any maintenance operations -- such as copying, reorganizing, cataloging, and scratching -- on RACF-protected group resources
- **Group-REVOKE**, which prevents the user from accessing resources as a member of the group and from making use of the other group-attributes

Figure 3 illustrates, in the non-shaded area, how a user in Group A who has a group-related user attribute in Group A can thus affect the resources and/or profiles associated within Group A and its subgroups, Group A1 and Group A2. (This example assumes that Group A is the owner of GROUP A1 and GROUP A2.) Note that this user cannot affect resources and/or profiles associated with Group B.

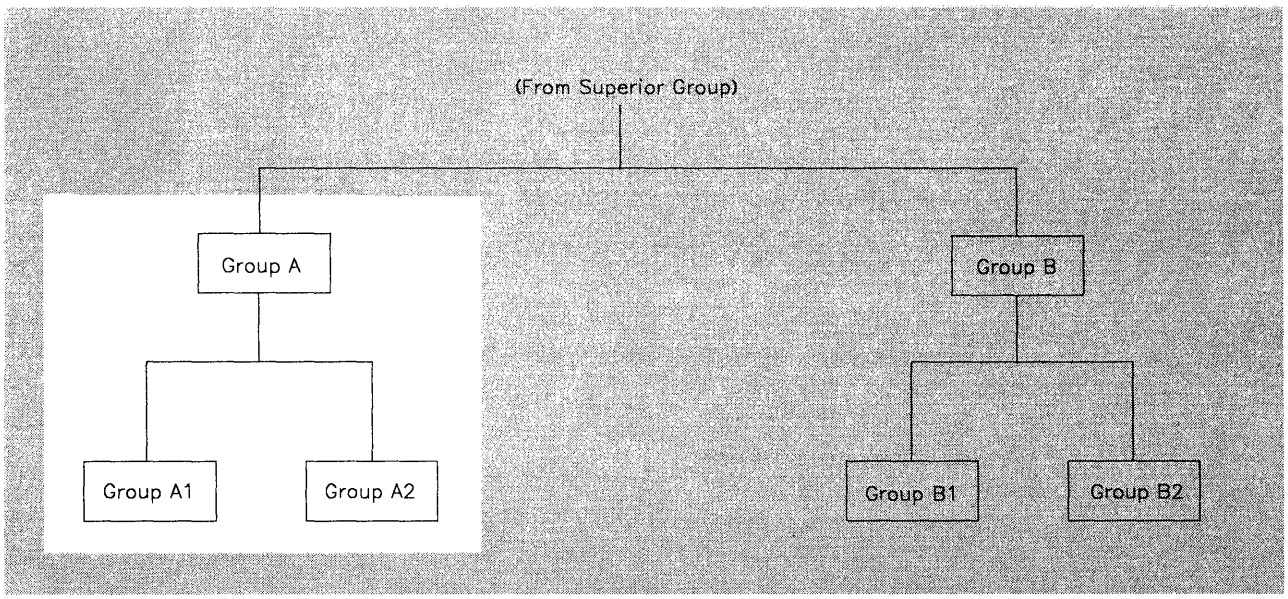

Figure 3. RACF Group-Related Attribute Control

Protecting Resources

In the same way as it defines users, an installation defines the resources it wants to protect. RACF protects both DASD and tape data sets, as well as other resources that are called "general resources."

On an **MVS system**, the types of general resources that RACF can protect include:

- DASD volumes
- Tape volumes
- Load modules (programs)
- IMS/VS transactions
- IMS/VS transaction groups
- IMS/VS application groups
- CICS/VS transactions
- CICS/VS started transactions (see Note 1)
- CICS/VS scheduled program specification blocks (PSBs)
- CICS/VS files (see Note 1)
- CICS/VS journals (see Note 1)
- CICS/VS programs (see Note 1)
- CICS/VS transient data destinations (see Note 1)
- CICS/VS temporary storage definitions (see Note 1)
- Applications (such as IMS/VS, CICS/VS, and Data Base 2)
- Terminals
- Installation-defined resources

Notes:

1. Your installation must have CICS/OS/VS Version 1 Release 7 installed to be able to protect these resources. In addition, this level of access control applies only to programs written using command level programming.

2. All of the CICS/VS resources also have groups.

On a **VM system**, the types of general resources that RACF can protect include:

- Minidisks
- Terminals
- Spool readers
- Nodes
- VM batch subsystem

RACF maintains **data set profiles** that contain security information about DASD and tape data sets, and **general resource profiles** that contain security information about general resources. These resource profiles include:

- The resource name and resource owner.

- The default level of authority -- universal access authority -- allowed for all users not specifically defined in the resource profile .

- A list of all the authorized users and groups, with their access authorities, called an **access list**.

- The **security classification** of the resource. The security classification includes one or more categories and a security level.

- Auditing options.

Each RACF-defined resource has a profile, though an installation can optionally use a single profile to protect multiple resources. Figure 4 illustrates a data set profile. A general resource profile is very similar.

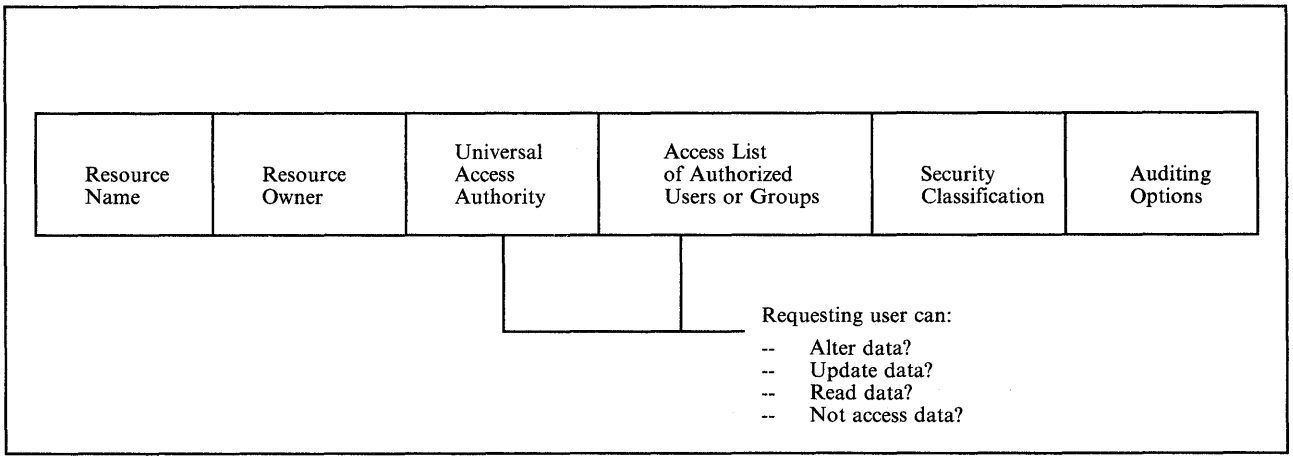

Figure 4. Key Fields in a Data Set Profile

The **security classification** consists of two types of information about the resource. The first is the categories that the resource belongs to. A **category** is an installation-defined name corresponding to a department or area within an organization with similar security requirements. A **security level** is an installation-defined name that corresponds to a numerical security level (the higher the number, the higher the security level).

When a user requests access to a resource that has a security classification, RACF performs two checks. The first check is a comparison of the security level in the user and resource profiles. If the resource has a higher security level than the user, RACF denies the request. The second check is a comparison of the list of categories (installation-defined names corresponding to departments or areas within an organization) in the user's profile with the list of categories in the resource profile. If the resource profile contains a category that is not in the user's profile, RACF denies the request.

If security classification checking does not deny access to the RACF-protected resource, then users and groups can be granted or denied access to the RACF-protected resource explicitly, by assigning each user or group a specific access authority to the resource, or implicitly, with a **universal access authority** (UACC).

The UACC is the default **resource access authority**. All users or groups of users in the system who are not specifically named in an access list of authorized users for that resource can still access the resource with the authority specified by the UACC. The UACC also applies to users not defined to RACF. The resource access authorities for data sets are:

- **ALTER**, which specifies that the user or group has full control over the resource. For minidisks on VM systems, the user or group has multi-write authority.
- **CONTROL**, which on MVS systems is used only for VSAM data sets, and specifies that the user or group has access authority that is equivalent to the VSAM control password. On VM systems, the user or group has multi-read authority.
- **UPDATE**, which specifies that the user or group is authorized to access the resource for the purpose of reading or writing.
- **READ**, which specifies that the user or group is authorized to access the resource for the purpose of reading only.
- **NONE**, which specifies that the user or group is not permitted to access the resource.

Types of RACF Profiles

RACF provides for three kinds of resource profiles -- discrete, generic, and grouped.

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 should be used for sensitive resources.

Generic profiles have a one-for-many relationship. One profile controls access to one or more resources whose names contain patterns or character strings that RACF uses to associate them with each other. For example, all data sets that have a high-level qualifier of WINTERS and the characters DIV02 as a second-level qualifier can be controlled with one generic profile.

The advantage of generic profiles is that the administrative effort is reduced in controlling access to a large number of resources that have similar names and the same access list, and this can result in a smaller RACF data set. In addition, if they are used properly, generic profiles can result in better performance because of reduced I/O activity (once generic profiles are loaded into main storage, they remain there as long as possible).

The third type of RACF profile is the grouped profile. Grouped profiles also have a one-for-many relationship, but there may be no way to associate the resources with a common access list based on patterns in the resource names. In this case, the many resource names can be associated with a single RACF profile through the use of a grouping profile that contains the names of the associated resources. Subsystems that have high performance requirements, such as IMS/VS and CICS/VS, have the profiles resident in the subsystem address space. These subsystems can save main storage by using grouped profiles.

RACF and the Operating System

To visualize how RACF works, picture RACF as a layer in the operating system that verifies users' identities and grants user requests to access resources.

Assume, for example, that a user has been identified and verified to the RACF-protected system, and now wants to modify an existing RACF-protected data set. After the user issues a command to the system to access the data set, a system resource manager (such as data management issuing OPEN in this example) processes the request. Part of the resource manager's processing, when RACF is active, is to "ask" RACF if this data set is protected, and, if it is, verify that the user can access it, and if requested, modify it. RACF checks various profiles to verify that the user can access the data set and to determine if the user has the required authorization to modify the contents. RACF then returns the results of its check to the resource manager. The resource manager, based on what RACF indicates, either grants or denies the request.

Figure 5 shows how RACF interacts with the operating system to allow access to a protected resource. The operating system-RACF interaction to identify and verify users is similar in approach.

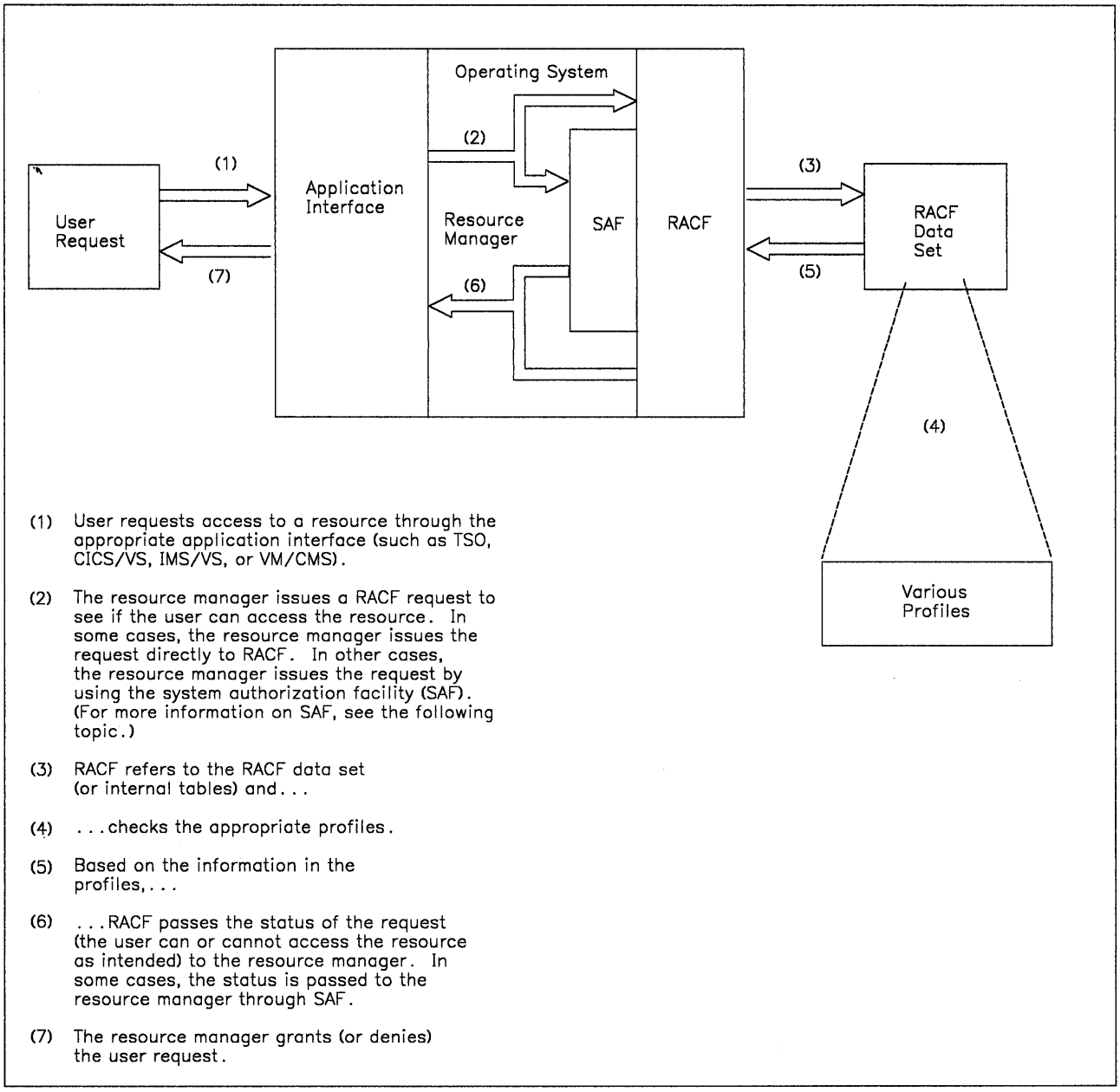

Figure 5. RACF and its Relationship to the Operating System

Figure 5 shows how RACF protects data by working with the operating system. RACF, during authorization checking, ensures that a user has the authorization to access the requested protected resource. RACF checks the resource profile to ensure, for example, that the resource can be accessed in the way requested and that the user has the proper authorization to access the resource. An analogy would be to the tumblers of a lock, all of which must align, before opening. In RACF, the necessary user-resource requirements must match before RACF grants the access request to a protected resource.

Figure 6 illustrates a **conceptual** model of how RACF checks profiles to ensure "who" (in a user profile) is accessing "what" and "how" (in a resource profile). Note that RACF may need to check some of the profiles only once, or RACF

may obtain data from a profile and refer to that data after moving it to another storage location. The important concept is that RACF ensures that the proper user-resource relationships exist before it allows a user to access a protected resource.

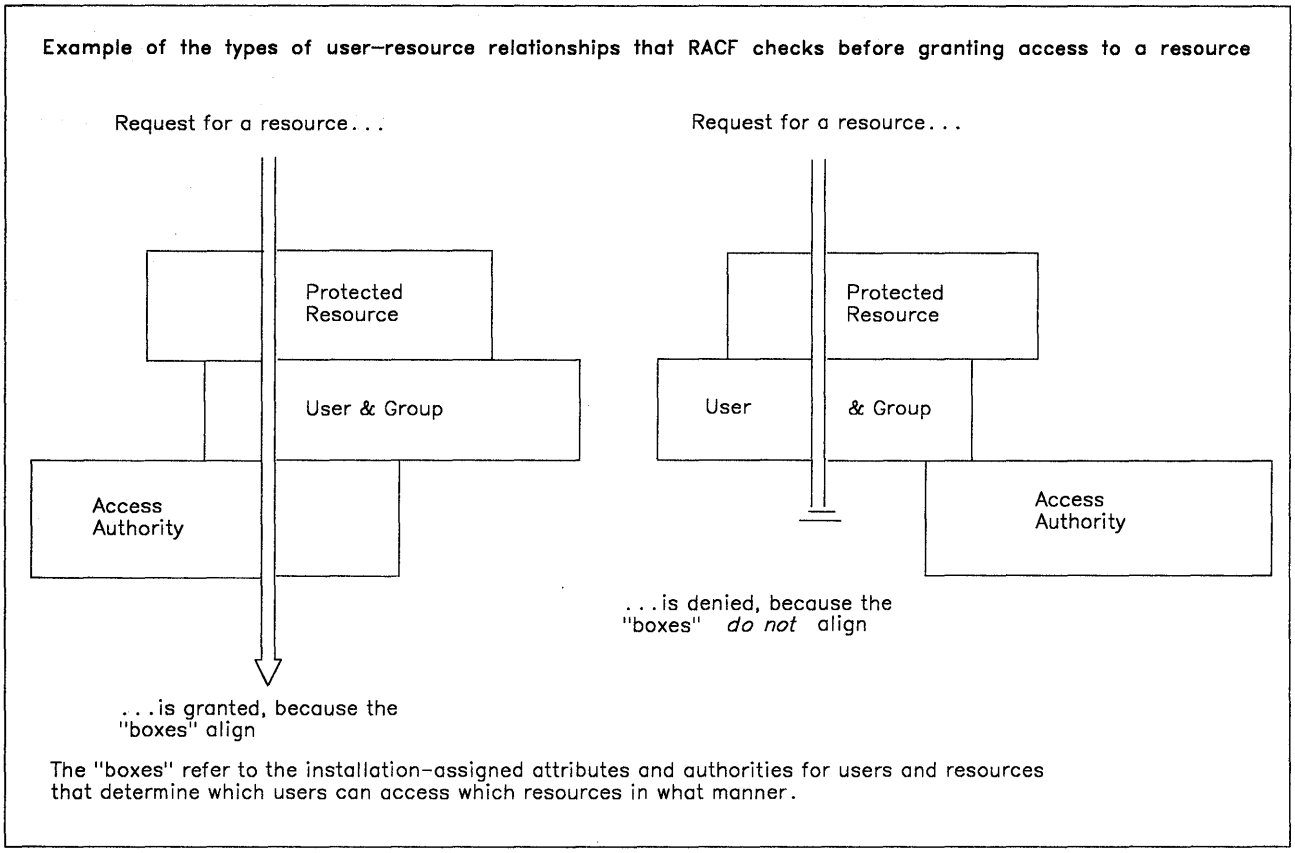

Figure 6. Conceptual Illustration of RACF Profile Checking

System Authorization Facility (MVS Systems Only)

The system authorization facility (SAF) is part of the MVS operating system and conditionally directs control to RACF, if RACF is present, and/or a user-supplied processing routine, when receiving a request from a resource manager. SAF does not require any other program product as a prerequisite, but overall system security functions are greatly enhanced and complemented by the concurrent use of RACF. The key element in SAF is the MVS router. The MVS router is always present in an MVS system, whether or not RACF is present.

The MVS router is a system service that provides a common focal point for all products providing resource control. This focal point encourages the use of common control functions shared across products and across systems. The resource managing components and subsystems call the MVS router as part of certain decision-making functions in their processing, such as access-control checking and authorization-related checking. These functions are called "control points."

In many cases, the resource manager (for example, data management) does not issue the "RACF" macro directly to RACF. Instead, the resource manager issues a RACROUTE macro to the system authorization facility (SAF). (RACROUTE is a SAF macro that should be used to perform most RACF functions.) SAF checks to see if RACF is installed in the system and active. If it is, SAF issues the "RACF" macro (for example, RACHECK), which describes the user's request to RACF.

Note: The RACROUTE macro also provides support for applications running in 31-bit mode.

Chapter 2: What Functions Does RACF Perform?

RACF protects resources by granting access only to authorized users of the protected resources. To accomplish this, RACF provides these functions:

- Identification and verification of users entering the system
- Authorization checking, to ensure that users can perform a requested action
- Logging and reporting
- Administrative control through the definition of profiles that describe the users and resources

On MVS systems, RACF provides additional support for these major functions with:

- Support for interaction with IMS/VS
- Support for interaction with CICS/VS
- Support for applications to use the RACF macros

User Identification and Verification

For a software access control mechanism to work effectively, it must be able to first **identify** the person who is trying to gain access to the system, and then **verify** that the user is really that person.

RACF identifies and verifies users accessing the system when the various system resource managers (such as job initiation) issue the RACINIT macro instruction. After a resource manager issues the RACINIT macro, RACF determines:

- If the user is defined to RACF
- If the user has supplied a valid password (and/or operator identification card) and group name
- If the user has the REVOKE attribute, which prevents a RACF-defined user from entering the system at all or entering the system with certain groups
- If the user can use the system on this day and at this time of the day (an installation can impose restrictions)

- If the user is authorized to access the terminal (which can also include day and time restrictions for accessing that terminal)
- If the user is authorized to access the application

Identification

RACF uses the userid in conjunction with a stored (and optionally encrypted) **password** to perform its user identification and verification. When an installation initially defines a user to RACF, the installation assigns a userid and temporary password. The userid identifies the user to the system as a RACF user. The temporary password permits initial entry to the system, at which time the user specifies a new password that cannot be retrieved.

Note: During terminal processing on MVS systems, RACF allows the use of an operator identification card (OIDCARD) in place of or in addition to the password. (The OIDCARD information can also be encrypted when stored on the RACF data set.)

Verification

When RACINIT processing verifies the user's identity, RACF specifies (in a control block called the accessor environment element, or ACEE) the scope of the user's authorization for the current terminal session or batch job. If RACINIT processing cannot verify the user identity during a terminal logon, the user is prompted (except for TSO users in no-prompt mode) for a valid password, operator identification card (MVS only), or group name (MVS only). In the case of an MVS batch job, the batch job fails. (However, if you have the JES support, JES propagates the current RACF userid from each already validated RACF user who is submitting a batch job to JES via the JES internal reader. This propagation eliminates the need for a userid and password on the JOB card.)

RACF provides installation exits that an installation may use during RACINIT processing.

Authorization Checking

Once it has identified and verified the user, RACF then controls interaction between the user and the protected resources. It must **authorize** not only what resources that user may access, but also in what way the user may access them (such as to read only or to update). After a resource manager issues the RACHECK macro, RACF performs authorization checking.

Figure 7 illustrates an example of RACHECK processing. The resource managers issue the other RACF macros in a manner similar to that illustrated for RACHECK.

Note: In some cases, the resource manager (for example, data management) does not issue the RACHECK macro directly to RACF. Instead, the resource manager issues a RACROUTE macro to the system authorization facility (SAF). (RACROUTE is a SAF macro that should be used to perform most RACF

functions.) SAF checks to see if RACF is installed in the system and active. If it is, SAF issues a RACHECK macro, which describes the user's request to RACF.

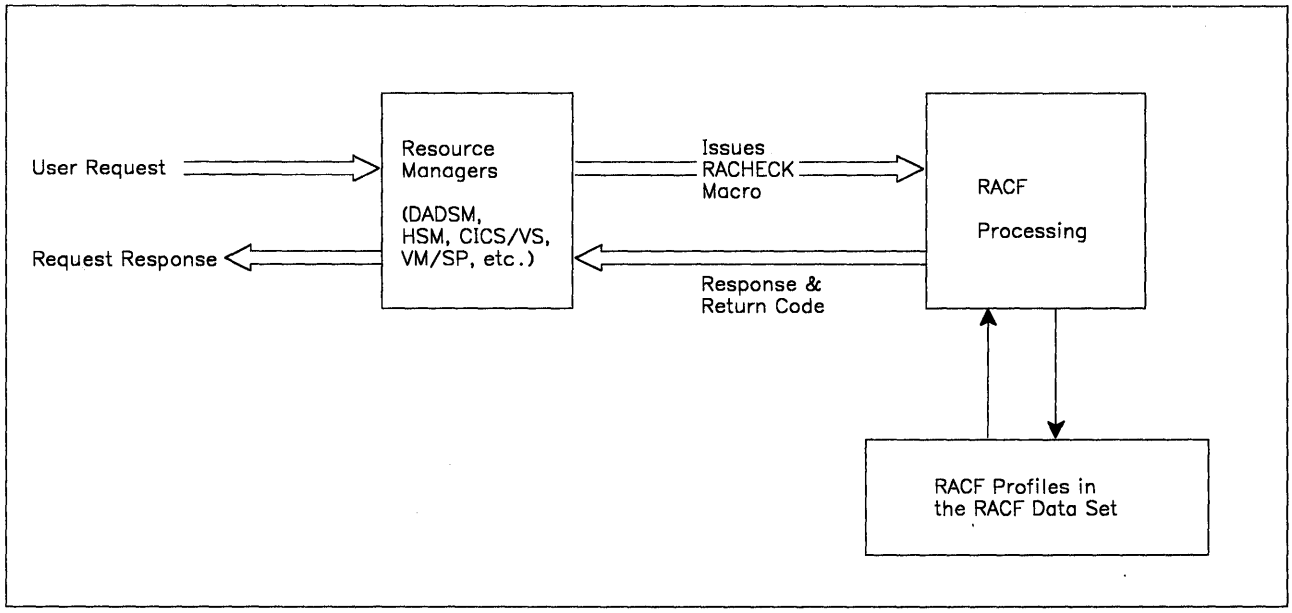

Figure 7. Example of RACHECK Processing

RACHECK processing determines if the user is authorized to access the resource. RACF checks the profiles to determine whether or not the conditions are met. If RACF determines that the user is not authorized to access the resource, the request is denied.

At the start of RACHECK processing, RACF does two checks that are related to the security classification of users and data. The first check is a comparison of the security level in the user and resource profiles. If the resource has a higher security level than the user, RACF denies the request. The second check is a comparison of the list of categories (installation-defined names corresponding to departments or areas within an organization) in the user's profile with the list of categories in the resource profile. If the resource profile contains a category that is not in the user's profile, RACF denies the request.

If RACF has not denied the request because of the security classification checks, RACHECK processing continues. RACF permits access to the resource if the user satisfies any of a number of conditions, such as:

- The resource is a data set and the high-level qualifier is the user's userid.
- The user's userid is in the access list with sufficient authority.
- The user's current connect group is in the access list with sufficient authority.
- When list-of-group checking is active, one of the other groups that the user is connected to is in the access list with sufficient authority.
- The universal access authority (UACC) is sufficiently high.

- The user has the OPERATIONS attribute (or the resource is within the scope of a group in which the user has the group-OPERATIONS attribute) and the user's userid or any group name the user is connected to is not in the access list with an authority less than the user's intended access.

RACF provides two installation exits that an installation may use during RACHECK processing, as well as a quicker form of authorization checking called "fast path RACHECK" (FRACHECK) processing.

RACF also provides global access checking. Global access checking allows an installation to establish a system-wide in-storage table of default authorization levels for selected resources. RACF checks this table to determine if access to a resource is permitted. If it is, RACF bypasses further RACHECK processing. If global access checking cannot permit access to the resource, RACHECK processing continues. Frequently-accessed resources with generalized access rules are good candidates for global access checking.

Global access checking handles resources in both the DATASET and the general resource classes, with the exception of group resource classes. The characteristics of global access checking are:

- Grants access, but does not, by itself, deny any request for access
- Allows no logging of permitted access and gathers no statistics
- Offers no postprocessing installation exit
- Does no I/O to the RACF data set, thus offering a high-performance checking option

The SETROPTS command controls global access checking for a specified class (or for all classes) and refreshes the global access checking table. The RDEFINE and RALTER commands establish and maintain the global access checking table entries. You can use the RLIST command, or the data security monitor (MVS only), to list the table's contents.

Logging and Reporting

RACF logging and reporting can help an installation detect possible security exposures or threats. RACF writes security log records for detected unauthorized attempts to enter the system and, optionally, for detected authorized or unauthorized attempts to access RACF-protected resources or to issue RACF commands. An installation can then list the contents of these records using the RACF report writer.

On an MVS system, RACF does the logging by writing SMF (system management facilities) records. On a VM system, RACF does the logging to a CMS file.

For detected, attempted security violations on the system, RACF also sends messages to the security console. RACF immediately reports events such as detected unauthorized attempts to enter the system and, optionally, detected

unauthorized attempts to access RACF-protected resources or modify the contents of the RACF data set. Optionally, on an MVS system, RACF can also notify a specified user of an unauthorized attempt to access a resource.

RACF maintains statistical information, such as the date, time, and number of times that a user enters a system and the number of times a specific resource was accessed by any one user. An installation can use this information to help analyze and more effectively control its computer operations.

Protecting Resources with RACF

RACF protects data sets (both DASD and tape) and general resources, such as tape volumes, VM minidisks, and terminals. RACF protects these resources through the profiles that an installation defines for the resources. Authorized users can create, modify, list, and delete profiles with RACF commands.

Profiles can be either generic or discrete; the choice depends on the nature of the resource. A **generic profile** can protect a single resource (such as one data set) or a number of related resources (that is, resources having similar naming structures and the same access-authorization and auditing requirements).

A **discrete** profile protects a single resource, and should be created when a certain resource, such as a single, sensitive data set on a specified volume, has specific or unique access-authorization or logging requirements. A data set protected with a discrete profile is always **RACF-indicated**, which means that an indicator is set to show that the data set must have RACF protection. (All other resources, such as IMS/VS transactions and VM minidisks, are not RACF-indicated.)

Protecting Data Sets

When you use the ADDSD command to define and protect a data set, RACF builds a data set profile and stores it in the RACF data set. If the access-authorization requirements are general, define a generic profile; if the data set has unique access-authorization requirements, define a discrete profile.

Generic Profile: A generic profile contains a list of the authorized users and the access authority of each user. A single generic profile can protect many data sets that have a similar naming structure. Data sets protected by generic profiles do not have to be defined individually to RACF, thus saving you much time that would be spent entering and maintaining individual profiles.

Figure 8 illustrates some valid generic profile names and the resource names that they match.

In general, a % in the generic profile name indicates that any single character in that same position of a data set name is a match. An * in the generic profile name indicates that any character in that position of a data set name, and all subsequent characters in that qualifier, are a match. In addition, if an * is the last character in the generic profile name, any subsequent qualifiers in the data set name are also considered a match.

Many users are able to protect all of their data sets by using a single generic profile consisting of their userid and an asterisk (userid.*). This profile protects all of the user's data sets that begin with the user's userid, regardless of the number of qualifiers. See the first example in Figure 8.

Notes:

1. Generic profile names do not always contain an * or a %, as shown in the last example in Figure 8.

2. If your installation has **always-call** support (your installation has installed RACF Version 1 Release 5 or later, and one of the following: MVS/370 Data Facility Product Release 1.1, MVS/XA Data Facility Product Version 1 Release 1.2, or MVS/XA Data Facility Product Version 2 Release 1.0) RACF is always called to determine if a resource is protected. To reduce the level of I/O activity from the calls to RACF, installations should use generic profiles extensively, with each profile protecting several data sets.

Generic Name	Resource Names Matched by the Generic Name
SEFCIK.*	SEFCIK.MEMO SEFCIK.MEMO.TWO SEFCIK.REPORT.WEEKLY
DPT44.*	DPT44.GROUP1 DPT44.GR.DATA
DPT44.*.DATA	DPT44.DEF.DATA DPT44.GROUP1.DATA
DPT44.GROUP*.XYZ	DPT44.GROUP1.XYZ DPT44.GROUP10.XYZ
DPT44.*.DAT*	DPT44.D.DAT DPT44.JMP.DATA1A DPT44.DEF.DAT.GBR DPT44.DPT04.DATA.GPB.RHG
DPT04.*.%%01	DPT04.DEF.GB01 DPT04.GROUP1.GR01
DPT44.DATA	DPT44.DATA (regardless of volume)

Figure 8. Examples of Generic Profile Names

Discrete Profile: A discrete profile contains the same kind of information as a generic profile, but it protects only the one identified data set on the specified volume or volumes. Data sets can be protected with discrete profiles in the following ways:

- Automatically, when users who have the ADSP (automatic data set protection) attribute create a permanent data set
- When users specify the PROTECT operand on the JCL DD statement or on the TSO ALLOCATE or access method service DEFINE commands for new permanent data sets
- When users issue the ADDSD command without the GENERIC operand for existing permanent data sets

Either type of profile 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 via an installation-supplied prefix

RACF can also protect data sets that are password-protected. If the data set is password-protected, the user must supply the password when creating a discrete profile. When a password-protected data set is also RACF-protected, access to the data set is determined only by RACF processing; password processing is bypassed. (A installation-written exit routine can modify RACF, however, so passwords can be used with RACF.)

RACF protection, however, has an advantage over password protection. With RACF protection, only authorized users can access the data set. With password protection, any user who knows the password can access the data set. Also, users can run jobs more easily with RACF protection because the system does not prompt the operator for data set passwords for RACF-protected data sets accessed during a job.

Protecting General Resources

When a user defines and protects a resource that is not a DASD or tape data set (via the RDEFINE command), RACF builds a general resource profile. Like profiles for data sets, general resource profiles can be generic or discrete. The general resource profile contains information about the resource, such as class name, resource name, and which attempts, successes or failures, are to be logged. It also contains a list of all the users or groups that are authorized to access the resource.

Note: For a list of the general resource classes, see "Protecting Resources" in Chapter 1.

Resource Classes

RACF recognizes a class of resources as those resources that are similar to each other. A tape volume, regardless of its contents or physical location, represents, for example, a specific way of storing data; tape volumes are a resource class. As another example, terminals might have different physical attributes, but they all perform similar input/output functions; terminals are a resource class.

Defining Resource Classes, Groups, and Members

An MVS installation can define resource classes in addition to the ones listed in Chapter 1. When an installation defines 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, and the location of the auditing and statistics flags for the class. An installation must supply the necessary control information for any new classes it defines. (RACF supplies the control information for the predefined resource classes.)

When defining a new resource class, an installation may optionally designate that class as either a resource **group** class or a resource **member** class. For a resource group class, any user or group of users permitted access via a profile for that resource group is permitted access to all members of that profile. Note that, for each resource group class created, a second class representing the members of the group must also be created. (GIMS and TIMS are an example of a resource group class and its respective resource member class.)

RACF uses the class descriptor tables whenever it makes a class-related decision (such as, "Should auditing be done for this class?"). On an MVS system, the class descriptor tables and the appropriate use of RACF authorization checking services (RACF macros) can extend RACF protection to any part of the system.

Protection with RACF Disabled (Failsoft Protection)

RACF, even when partially disabled in a system, provides some protection and offers default services. RACF can use various internal tables to verify requests for protected resources, can route control to various exit routines for further processing, and can log the requests, whether they are granted or denied.

RACF and IMS/VS (MVS Systems Only)

RACF provides IMS/VS user verification, IMS/VS transaction authorization, and user authorization to the IMS/VS application. If an installation specified the RACF option during SYSGEN, IMS/VS issues the RACLIST macro instruction at IMS/VS START, RESTART, and for the command /MODIFY COMMIT. RACLIST builds a resident profile for each IMS/VS transaction defined to RACF, either individually or as a member of a group.

User Verification

RACF user verification is invoked when an IMS/VS user enters the SIGN ON command. The RACINIT macro instruction verifies:

- The validity of user identification
- The specified user password
- Authorization to the specified group (if any)
- A new password (if any)
- Authorization to IMS/VS
- Authorization to the physical terminal

If the user is verified, RACINIT processing returns the address of the user's ACEE. IMS/VS also invokes user verification to perform cleanup when a user enters SIGN OFF or enters a new SIGN ON command without first signing off a previous session.

Authorizing Users Who Have Not Signed On

RACF builds the IMS/VS user's ACEE (accessor environment element) only when the user issues SIGN ON to IMS/VS. For the user who does not sign-on and has no unique ACEE, all transaction authorization is based on the ACEE associated with the IMS/VS control region.

Transaction Authorization

Transaction authorization involves checking the in-storage profiles built by RACLIST to determine if a user or group is authorized to execute the transaction. IMS/VS invokes RACF transaction authorization checking on each:

- Transaction input from a terminal
- Change call to a modifiable IMS/VS program control block (PCB)
- /SET command
- /LOCK TRAN command
- /UNLOCK TRAN command
- Insert of a scratch pad area containing a transaction name

If the transaction has not been defined to RACF, IMS/VS considers the transaction to be unprotected by RACF.

User Reverification

RACF provides a further security check known as user reverification for IMS/VS transactions or transaction groups. During user reverification, the user enters a password along with the transaction. RACF checks this password against the user password entered at SIGN ON to ensure that the transaction is being executed by the user RACF originally verified at SIGN ON.

For more information, see Chapter 7 of the *RACF Security Administrator's Guide*.

Application Group Name Checking

IMS/VS uses RACF to control access to resources that are under control of the online system. To prevent an unauthorized user from starting a batch message processing (BMP) region and accessing online resources through the parameter statement on the EXECUTE card, IMS/VS will issue a RACHECK specifying the application group name (AGN) to RACF. The AGN name must have been specified in the EXECUTE card parameter list for the BMP if IMS/VS is using this option. If the AGN name is defined to RACF in the proper class (usually AIMS), and if the user starting the BMP is authorized access to the application group name, IMS/VS then checks to see if the PSB, TRAN, or LTERM name in the other parameters is defined under that name in the IMS/VS security matrix.

If either of these conditions is not met, IMS/VS does not schedule the BMP region.

RACF and CICS/VS (MVS Systems Only)

When the command level interface is used, RACF can provide services related to access control for all resource types formerly protected by CICS/VS resource security level checking.

RACF services can replace the CICS/VS sign-on table, thus allowing terminal users to manage their own passwords. In addition, the use of RACF services can simplify the administration of access control and relieve the CICS/VS system programmer of some of the activities associated with maintaining security-related information in the tables that describe the CICS/VS resources.

User Identification and Verification

CICS/VS invokes the RACINIT service, during execution of the sign-on transaction, to identify and verify the user, allow changing of the user's password, require changing of the user's password after the password expires, and revoke the user's access to the system if the user does not provide a correct password in the last 'n' tries.

The RACINIT service also checks to see if the user is authorized to access that particular CICS/VS system, and whether the user is authorized to use that terminal.

If the user is authorized, the RACINIT service builds an ACEE for that CICS/VS task, and points to this control block in a field specified by CICS/VS. This control block contains the user's identifier and the RACF groups to which the user is connected. Subsequent access control checking service requests issued by CICS/VS will point to this control block.

Resource Authorization Checking

When an application program requests a CICS/VS resource through the command level interface, CICS/VS checks whether the requested resource is RACF-protected. If it is, CICS/VS asks RACF to determine whether the request is authorized. To do this, CICS/VS prepares a call to the fast RACHECK (FRACHECK) service routine, specifying the RACF resource class, the name of the requested resource, and the location of the RACF ACEE that was built when the user signed-on. RACF scans an index to profiles that was loaded when CICS/VS was initiated, locates the profile, and determines whether or not the user is authorized to access this resource. RACF then returns a code to CICS/VS to indicate whether the user is authorized. If the user is not authorized, CICS/VS sends a message to the terminal, terminates the transaction, logs the violation in the CSCS transient data destination, and issues a RACHECK which causes RACF to write an SMF record.

The classes of resources that CICS/VS protects via RACF are:

- Transactions
- Started transactions
- Scheduled program specification blocks (PSBs)
- Files (data sets)
- Journals
- Programs
- Transient data destinations
- Temporary storage definitions

It is likely that not all CICS/VS installations will want to control access to all classes of resources, nor all resources in any given class. For example, if transactions are written to be very specific as to what they do, transaction control is probably adequate. If transaction processing programs are not specific in their intent, it might be desirable to control access to the files, rather than to the transactions or the programs.

CICS/VS uses the RACLIST service of RACF at system initialization time to bring its resource profiles into main storage. The profiles are brought into main storage to provide maximum performance during security checking. If the access lists of the resource profiles contain RACF group names that represent job descriptions, there should be no reason to refresh these profiles because RACF group affiliations are established at sign-on time, and RACF administrators can change these affiliations very easily. However, if it is necessary to refresh the in-storage profiles, execute the CICS/VS CEMT PERFORM SECURITY REBUILD transaction.

For more information on how to invoke RACF services from CICS/VS, see Chapter 8 of the *RACF Security Administrator's Guide*.

RACF Generalization

RACF generalization allows applications to use the RACF macros for identification, verification, and authorization functions. Applications can use the "RACF" macros that are part of MVS, as well as the macros that are part of the RACF program product.

Some of the macros that RACF uses are part of MVS and not part of RACF itself. MVS installations receive these macros even if they do not install RACF. These macros are:

- **RACDEF** - used to define, modify, or delete resource profiles for RACF.
- **RACHECK** - used to provide authorization checking when a user requests access to a RACF-protected resource.
- **FRACHECK** - used to provide authorization checking when a user requests access to a RACF-protected resource (similar to RACHECK). However, FRACHECK verifies access to only those resources that have RACF profiles brought into main storage by the RACLIST facility.

- **RACINIT** - used to provide RACF user identification and verification.
- **RACLIST** - used to build in-storage profiles for RACF defined resources.
- **RACROUTE** - used to invoke the system authorization facility (SAF) MVS router. The RACROUTE macro provides the functions of RACDEF, RACHECK, RACINIT, RACLIST, RACXTRT, and FRACHECK. RACROUTE also provides support for applications running in 31-bit mode.
- **RACSTAT** - used to determine if RACF is active and optionally to determine if RACF protection is in effect for a given resource class. The RACSTAT macro can also be used to determine if a resource class name is defined to RACF.
- **RACXTRT** -used to retrieve specified fields from a resource profile or to encrypt data.

RACDEF, RACHECK, RACINIT, RACLIST, RACROUTE, and RACXTRT are fully documented in *OS/VS2 SPL: Supervisor* and *MVS/XA SPL: System Macros and Facilities*. RACHECK and RACROUTE are also documented in *Supervisor Services and Macro Instructions* (both MVS/370 and MVS/XA). FRACHECK and RACSTAT are fully documented only in *Supervisor Services and Macro Instructions* (both MVS/370 and MVS/XA).

The macros that are part of the RACF product are:

- **ICHERCDE** - used to generate entries for the resource class descriptor table
- **ICHRFRTB** - used to generate entries in the RACF router table
- **ICHNCONV** - used to create the installation's naming convention table
- **ICHEINTY** - used to locate and/or update profiles on the RACF data set
- **ICHETEST** - used to test for user-specified conditions on selected fields in a profile on the RACF data set
- **ICHEACTN** - used to retrieve and alter specified fields within a profile on the RACF data set

All of these macros that are part of the RACF program product are described in *System Programming Library: RACF*.

Chapter 3: Using RACF

RACF protects critical system resources by allowing only the installation-defined users and groups to access those protected resources. To define the level of RACF protection and to control RACF processing, RACF provides:

- ISPF panels and RACF commands
- Processing options
- Tools for reporting and recording
- Installation exits

RACF panels (under ISPF) or RACF commands (under TSO or CMS) define the groups, users, and resources that an installation wants to protect. The RACF panels (or commands) are the primary method of user interaction with RACF.

An installation can specify options that define levels of protection and allow recording of access attempts to protected resources. The SETROPTS command enables and disables RACF processing options such as global access checking, generic profile checking, and password rule checking.

An installation can record statistics, list what users are identified to RACF, and generate security reports with the RACF tools and utilities. The RACF tools provide, in effect, better feedback and control of the use of RACF.

An installation can also define and write exit routines that RACF calls during certain operations. RACF works without these exit routines, but the "hooks" for the exit routines allow an installation to perform additional security checking and to tailor RACF to the installation's individual needs.

RACF ISPF Panels and Commands

The RACF panels (or commands) allow authorized users to perform the following functions:

- Define the users, groups, data sets, and general resources an installation wants to protect
- Create, modify, or delete user, group, data set, general resource, and connect profiles
- Maintain profile access lists
- List the contents of various profiles
- Define passwords

- Remove RACF-protection from resources
- Enable and disable various RACF options

To request these functions, a user can enter ISPF and use the RACF panels, submit the commands as a background job, or enter the commands interactively during a TSO or CMS session. Figure 9 shows an example of a RACF ISPF panel, the service option menu on an MVS system.

```
                          RACF - SERVICE OPTION MENU
OPTION===>

SELECT ONE OF THE FOLLOWING:

    1   DATA SET              ADD, CHANGE, DELETE, or DISPLAY the profile
                              for a data set.

    2   GENERAL RESOURCE      ADD, CHANGE, DELETE, or DISPLAY the profile
                              for a general resource.

    3   GROUP                 ADD, CHANGE, DELETE, or DISPLAY a group profile.
                              CONNECT or REMOVE users.

    4   USER                  ADD, CHANGE, DELETE, or DISPLAY a user profile.
                              Change a user's password.

    5   SYSTEM OPTIONS        DISPLAY or SET the system wide security options.
                              REFRESH in-storage profile lists.

    6   TUTORIAL              View a general description of RACF.
```

Figure 9. RACF Services Option Menu (on an MVS System)

Figure 10 lists the RACF commands and groups them by entity type (such as commands for general resources).

Appendix A explains the functions of the RACF commands. Appendix B lists the RACF commands and identifies the user authorities and attributes needed to issue the commands. If the user does not have the proper authority, RACF issues a message and does not complete the command request.

Data Set	General Resource	Group	User	Other
ADDSD	RDEFINE	ADDGROUP	ADDUSER	CONNECT
ALTDSD	RALTER	ALTGROUP	ALTUSER	PASSWORD
DELDSD	RDELETE	DELGROUP	DELUSER	PERMIT
LISTDSD	RLIST	LISTGRP	LISTUSER	REMOVE
				RVARY
				SEARCH
				SETROPTS

Figure 10. RACF Commands by Resource Type

RACF Options

An installation can specify many RACF options with the SETROPTS command or the system options RACF ISPF panel. Some of these options are:

- Global access checking
- Generic profile checking
- Tape data set protection (MVS/XA only)
- Requiring RACF-protection for all new data sets (MVS only)
- Erasure of all or selected DASD data sets as they are deleted (MVS/XA only)
- Activating program control (MVS/XA only)
- Statistics gathering
- Undefined terminal protection
- User password expiration and syntax rules
- Single-level data set name processing (MVS only)
- Bypassing automatic data set protection (MVS only)
- List-of-groups authority checking
- Data set modeling (MVS only)
- Use of real data set names in messages and SMF records (MVS only)
- JES options for RACF (MVS only)
- Logging of RACF events

These RACF options provide flexibility in the creation and administration of an installation's RACF security system. RACF options can effectively enhance performance and recovery.

Performance Options

RACF's effect on system utilization depends upon the type and number of RACF functions performed and the I/O activity to the RACF data set. RACF provides options to reduce and balance this I/O activity:

- By using resident index and data blocks, an installation can reduce the number of I/O requests to the RACF data set. This option is strongly recommended.

- By using the multiple RACF data set option, an installation can split the RACF data set into many RACF data sets across a number of devices. (On a VM system, the RACF data base can be split and spread across a number of devices.) This action can balance I/O activity by spreading the accesses across devices, thus reducing the possibility of device contention.

In addition to performance, this last option can also improve availability, because it reduces the number of resources made unavailable by the loss of one data set or device.

RACF provides other options that may, under certain conditions, improve system performance if they are used:

- The effective use of the generic profile checking facility, which allows the RACF SVCs to build resident profiles during access authorization checking, can enhance system performance by reducing the frequency of I/O requests. Generic profile checking can also reduce the size of the RACF data set and decrease administrative requirements, because a few generic profiles can protect a substantial number of resources. Otherwise, the installation would have to define each resource separately to RACF and store a unique discrete profile for each resource in the RACF data set.

- The use of global access checking can also improve system performance. With global access checking, an installation can bypass normal RACHECK profile processing in most cases, and instead use an in-storage table containing generalized access rules.

  Caution: If your installation has **always-call** support (your installation has installed RACF Version 1 Release 5 or later, and one of the following: MVS/370 Data Facility Product Release 1.1, MVS/XA Data Facility Product Version 1 Release 1.2, or MVS/XA Data Facility Product Version 2 Release 1.0) RACF is always called to determine if a resource is protected. To reduce the level of I/O activity from the calls to RACF, installations should use global access checking and generic profiles. Global access checking and generic profiles are very efficient because they use in-storage information.

- RACF statistics options allow a reduction of I/O activity to the RACF data set.

- RACF logging options allow a reduction of SMF (system management facilities) I/O activity by restricting logging to specified access levels to individual resources.

Automatic Backup for the RACF Data Set

RACF permits the installation to automatically maintain back-up copies of any RACF data set and to switch to those copies if the primary RACF data set is lost as a result of physical destruction or operational error.

RACF Tools

RACF provides a number of tools to help an installation monitor and control RACF events. These tools perform the following functions:

- Generate reports based on RACF logging records
- Record statistics in RACF profiles
- List the userids or group names found in the RACF data set.
- List information contained in the RACF profiles
- Report system integrity and security status

Generating Reports from Logging Records

The RACF report writer lists information derived from logging records that RACF generates. On an MVS system, these are SMF records. On a VM system, the information is in a CMS file.

The RACF report writer can generate reports that :

- List the contents of RACF logging records in a format that is easy to read, including using the real data set names (not the internal name given by an installation exit routine).
- Describe attempts to access a particular RACF-protected resource. These reports contain the user identity, the number and type of successful accesses, and the number and type of unauthorized accesses.
- List the warning messages RACF issues during the "grace" period (before RACF control is enforced).
- List resource activity by resource owner.
- List the resource owners.
- Describe user and group activity.
- Summarize system and resource use.

The user can request a general summary as well as many specialized summary reports.

Recording Statistics in RACF Profiles

RACF places the creation date into profiles when it creates them. In addition, RACF can also dynamically place into **discrete** profiles various statistics.

In data set and general resource profiles, RACF can optionally (depending on the RACF command options) record the following statistics:

- The date the resource was last referenced
- The number of times the resource was accessed under each RACF authority (such as READ or UPDATE)
- The number of times that a specific user or group accessed the resource
- The date the profile was last updated

For user profiles, RACF can optionally (depending on the RACF command options) record statistics such as:

- The date and time of the last RACINIT for a particular user
- The number of RACINIT macros issued for a particular group
- The date and time of the last RACINIT for a user to a particular group

These statistics enable you to examine the current operation of your system for administrative and control purposes. You can list the statistics and other

descriptive information recorded in RACF profiles by using various RACF commands, as described in a following topic, "Listing Information from RACF Profiles."

Listing Userids or Group Names Found in the RACF Data Set

RACF provides a utility program to list all occurrences of a userid or group name in the RACF data set. The utility program, ICHUT100, uses a RACF component called the RACF manager to access the RACF data set and locate the places where userids and group names are found.

Executing ICHUT100 requires that the user have the SPECIAL, group-SPECIAL, AUDITOR, or group-AUDITOR attribute. Users not having one of these attributes can, however, list occurrences of their own userid.

Listing Information from RACF Profiles

The commands described in Figure 11 permit a user to list the contents of profiles:

Command	Function
LISTDSD	Displays the contents of discrete or generic data set profiles. The output includes the owner of the profile, the universal access authority, the date the profile was created, the users and groups authorized to access the data set(s), your highest access authority to the data set, the security level, a count of the accesses to a data set with a discrete profile, and other information.
LISTGRP	Displays the contents of group profiles. The output includes the owner of the group profile, the superior group name, the users connected to the group, the subgroup names, and other information.
LISTUSER	Displays the contents of user profiles. The output includes the owner of the profile, the user name, the default group name, the groups that a user is connected to, group authorities, the security level, the date the password was last changed (but not the password itself), and other information.
RLIST	Displays the contents of discrete or generic profiles for general resources, such as tape volumes, DASD volumes, VM/CMS minidisks, and IMS/VS transactions. The output includes the owner of the resource, the date the resource was defined, the universal access authority, the users and groups authorized to access the volume, your highest access authority to the resource, the security level, a count of the accesses to a resource with a discrete profile, and other information.
SEARCH	Displays the resource names from the RACF data set. RACF bases the search for resource names on a "mask," a character string specified with the command. On MVS, a user can direct the output to a TSO CLIST data set.

Figure 11. Commands to List Profile Contents

The listings from the commands described in Figure 11 enable an installation to track and maintain control of all RACF-defined users, groups, and resources in its computing system.

Checking System Security (MVS Systems Only)

The data security monitor (DSMON) enables an installation to verify the basic system integrity and data security controls. RACF auditors can use the DSMON reports to evaluate the level of security at the installation. Using the data security monitor, an authorized user can create the following reports:

- **System report**, which specifies the model and identification number of the processor complex, the name and level of the system control program, the volume on which the system resides, and the system identifier that SMF uses. The system report also indicates whether or not RACF is active, and, if it is, the RACF version and release number. The system report is the only report that DSMON produces when RACF is inactive.

- **Program properties table report**, which lists all the programs residing in the program properties table. The program properties table report indicates which programs are authorized to bypass password protection, and which programs can run in a system key.

- **RACF authorized caller table report**, which lists all the programs in the RACF authorized caller table and specifies which programs are authorized to issue the RACINIT and RACLIST SVCs.

- **RACF exits report**, which lists the name and size (in bytes) of each installation-defined RACF exit routine.

- **Selected user attribute report**, which lists all the RACF users at the installation who have the SPECIAL, OPERATIONS, AUDITOR, or REVOKE attributes, and whether each user has these attributes at the system or group level.

- **Selected user attribute summary report**, which lists the number of users defined to RACF at the installation, as well as identifying the number of users defined to RACF with the SPECIAL, OPERATIONS, AUDITOR, and REVOKE attributes, at both the system and group level.

- **Selected data sets report**, which lists information about data sets selected according to criteria provided by DSMON and the user. The selected data sets report includes the data set name, the criterion for selection, the serial number of the volume it resides on, whether or not the data set is RACF-indicated, whether or not the data set has RACF protection, and the UACC of the data set.

- **Started procedures table report**, which lists, for each procedure in the started procedures table, the procedure name, the userid and group name to be associated with the procedure, and whether the procedure is privileged (all RACHECKs for that procedure are considered successful).

- **Class descriptor table report**, which lists, for each general resource class, the class name, the default UACC, whether the class is active, whether auditing is being done, whether statistics are being kept, and whether OPERATIONS attribute users have access.

- **Global access table report**, which lists, for each general resource class in the global access table, all the entry names and their associated global access checking authority levels.

- **Group tree report**, which lists, for each requested group, all its subgroups, all the subgroups' subgroups, and so on, as well as the owner of each group listed in the report.

Figure 12 illustrates a typical data security monitor report.

```
RACF DATA SECURITY MONITOR                    DATE:  04/05/85      TIME:  17:02:59
                    S E L E C T E D   U S E R   A T T R I B U T E   R E P O R T
USERID           -------------   ATTRIBUTE TYPE   ------------
                 SPECIAL         OPERATIONS      AUDITOR       REVOKE
-------------------------------------------------------------------------------
D09RHG1          GROUP           GROUP
D09GMB1          SYSTEM          SYSTEM          SYSTEM
D09ABL1          GROUP           GROUP
D58GBR1                                          SYSTEM
IBMUSER          SYSTEM          SYSTEM                        SYSTEM
SYSUSER          GROUP
```

Figure 12. Sample Data Security Monitor Selected User Attribute Report

Installation Exits and Tables

To tailor RACF or to perform additional security checking, an installation can write **installation exit routines**. RACF supports installation exit routines for use with:

- RACDEF, RACHECK, RACINIT, and RACLIST macro instructions
- FRACHECK processing
- Some commands
- Password processing
- RACF report writer

RACF also allows an installation to create a naming conventions table and a started procedures table. A naming conventions table helps an installation set up and enforce data set naming conventions that are different from the standard RACF naming conventions. The started procedures table allows a started procedure, such as JES, to access a RACF-protected resource.

For more information on these installation exits and tables, see *System Programming Library: RACF.*

Chapter 4: Planning for RACF

Data security, as described in Chapter 1, is defined as the protection of data from accidental (or deliberate) unauthorized disclosure, modification, or destruction. Based on this definition, it is apparent that all data processing installations have at least potential security or control problems. Users have found, from past experience, that data security measures can have a significant impact on operations in terms of both administrative tasks and demands made on the end user. This chapter provides some suggestions that might be useful in understanding who will use RACF, how to plan for RACF, and who will be involved in implementing RACF.

RACF gives the user defined with the SPECIAL attribute -- the security administrator -- a great many responsibilities (both at the system level and at the group level). Thus, the security administrator (assumed to be at the system level for the remainder of this chapter) is a logical choice to be the focal point for planning security at your installation. As the focal point for security, the security administrator's planning would probably include the following tasks:

- Determining which RACF functions to use
- Identifying which data RACF is to protect
- Identifying the level of RACF protection
- Identifying administrative structures

Determining the RACF Functions To Use

RACF provides many functions to help achieve the level of protection needed for your installation. Some of the factors that determine what functions to select are:

- Your installation's security objectives
- The security measures that already exist
- An evaluation of how RACF will help you reach your goals

Your installation, for example, may require security for part or all of its data base. You can use RACF to define and protect these parts. Your installation might want to limit the users who can access certain data, and make RACF "invisible" to other users. RACF provides a very flexible approach for defining which users can use which data; you define these restrictions with user attributes, group structures, and access authorities within group structures.

The key factor is to understand what RACF functions you want to use in order to achieve your security goals. The following list shows some RACF functions that you might use and relates these functions to the security they provide.

RACF Function	Security Provided
Data Set Protection	RACF can protect both DASD and tape data sets. Protection can be gradually phased in; new data sets can be easily and automatically protected. Existing data sets can also be protected.
Resource Protection	RACF can protect several classes of resources, such as minidisks, load modules, terminals, applications, tape volumes, and user-defined resources. Protection can be gradually phased in.
Naming Conventions	While implementation of RACF security for data sets is easier when your installation already has a consistent data set naming convention, a consistent data set naming convention is not a requirement. RACF provides a table to allow you to use your own data set naming conventions on an MVS system. You can also use installing RACF as an opportunity to implement consistent naming conventions.
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.
Group Names	RACF provides for group structures and userids. Groups can be based on the user functions performed, if desired.
Transparency	RACF can provide for end user transparency by techniques such as discrete profile modeling and generic profiles. On an MVS system, RACF can provide transparent protection for data sets that need discrete profiles.
RACF Tailoring	RACF provides installation exits for customizing RACF processing.
Recovery	RACF provides a controlled environment during recovery of the RACF data set.
Violation Detection	RACF provides violation detection through its logging, reporting, and auditing capabilities.
Subsystems	RACF can control the use of IMS/VS and CICS/VS resources.

Identifying the Data to Protect

Every installation has varying amounts of confidential data and varying degrees of confidentiality. Generally speaking, all data falls into one of the following categories:

1. Very sensitive/confidential data, which requires protection from any disclosure, modification, or destruction.

2. Non-confidential data, which is recoverable with little inconvenience if destroyed.

3. The vast amount of data that falls between these two extremes, which should be protected from inadvertent or deliberate modification or destruction.

Obviously, you **must** protect the data in the first category. What you should also consider is how to protect the data that **ought** to be protected in a simple yet effective manner, and achieve this protection with minimum impact on the end user.

The task of protecting large quantities of data can take on significant proportions unless you can acquire protection automatically. In the case of new data, it is

quite simple and, once the controls are in place, practically free from administrative overhead.

Protecting New Data Sets (MVS Systems)

RACF provides several ways to protect new data sets automatically. When generic profile checking is active, new data sets are automatically RACF-protected if the data set name matches an existing generic profile name. You can also automatically RACF-protect data sets by assigning the ADSP attribute to the user, or by using the PROTECT operand on the JCL DD or TSO ALLOCATE statements for the data set. You can also combine profile modeling with this process. (See the next topic for more information.) However, ADSP and PROTECT force the creation of a discrete profile; you should use discrete profiles only for data sets that have unique access-authorization requirements.

You provide protection (but not automatically) for any new data set with the RACF ADDSD command (or the DATA SET series of panels). To enforce RACF-protecting new data sets, RACF has a "protect-all" option (on the SETROPTS command). The protect-all option allows a user to create a data set only when the data set will be RACF-protected by either a discrete or generic data set profile.

Notes:

1. Tape data set protection is not in effect when you install RACF. Your installation must issue the SETROPTS command with the TAPEDSN option, as well as activate the TAPEVOL general resource class, to activate tape data set protection.

2. Tape data set protection is available only on MVS/XA systems that have Data Facility Product Version 2 Release 1 installed.

3. Unless an installation has **always-call** support (your installation has installed RACF Version 1 Release 5 or later, and one of the following: MVS/370 Data Facility Product Release 1.1, MVS/XA Data Facility Product Version 1 Release 1.2, or MVS/XA Data Facility Product Version 2 Release 1.0), DASD data sets must be RACF-indicated in order for RACF protection to be in effect.

Profile Modeling

Profile modeling enables RACF or an installation exit routine to copy information (such as the access list, owner, logging options, and so forth) from an existing profile when defining a new profile. This copying greatly reduces the effort needed to create new profiles.

An installation can establish profile modeling either with a RACDEF preprocessing installation exit routine or with the SETROPTS command. The MODEL operands of the ADDUSER, ADDGROUP, ALTUSER, and ALTGROUP commands allow users to automatically supplement the information normally placed in new RACF data set profiles created by ADSP, PROTECT=YES, or ADDSD.

RACF also allows a user to specify an existing profile name on the ADDSD and RDEFINE commands, that RACF uses as a model when creating the new profile. Keywords on these commands enable the user to copy all the information from an existing profile.

Protecting Existing Data Sets (MVS Systems)

Existing data sets can be protected by either discrete or generic profiles. The use of generic profiles can decrease the administrative cost because a single generic profile can protect a large number of existing data sets that have a similar naming structure.

A tape data set created before the activation of tape data set protection is protected by the existing TAPEVOL profile. A tape data set created after the activation of tape data set protection is protected by a profile in the DATASET class, even if the volume was already protected by a profile in the TAPEVOL class.

Note: Unless an installation has **always-call** support (your installation has installed RACF Version 1 Release 5 or later, and one of the following: MVS/370 Data Facility Product Release 1.1, MVS/XA Data Facility Product Version 1 Release 1.2, or MVS/XA Data Facility Product Version 2 Release 1.0), DASD data sets must be RACF-indicated in order for RACF protection to be in effect.

Protecting Other Data

Besides protecting the data in DASD and tape data sets, RACF can also protect other resources, including minidisks, DASD volumes, tape volumes, and load modules.

Note: On a VM system, use the VMMDISK class to protect minidisks.

Identifying the Level of Resource Protection

RACF allows you to specify different levels of protection for your resources, and to gradually "increase" the level of RACF protection. In all cases, you can use RACF to report about access to the resources. You can:

- Allow access to resources without denying access to those resources, and log and report user access to the resources.
- Issue and log warning messages about user access to resources that would normally be denied, but allow access for a limited time. This is called the "grace period," and you can use the grace period to begin RACF protection without denying access until a later date.
- Provide full RACF protection to your resources and log and report both successful and unsuccessful access attempts.

Identifying Administrative Structures

Your organization's data access patterns are probably well established by department and/or function. You can regard each department or function as a group and define these groups to RACF. Groups are the key element in your RACF scheme, and the underlying security requirement tends to be for group isolation. You can make group isolation automatic and transparent to end users. Group isolation is easy to implement and gives a wide base on which to refine your security controls. A RACF group also serves as a focal point for delegating authority to users within the group and for controlling the data sets associated with it the group.

Identifying Your User and Group Relationships

Identifying and defining user and group relationships makes it simpler and more efficient to protect resources that those users and groups create, share, or use. In instances where some groups require exceptional access controls, you might sub-divide your organization to minimize occasions when data needs to be passed between these groups and the rest of the organization. If the users in a group share common access requirements, as is often the case, the administrative task of authorizing users is greatly simplified. In your installation it might be enough to simply isolate development work from production. On the other hand, it might be practical to isolate many individual users and groups. In either case, you must arrange the groups in a structure to form a hierarchical tree so that each RACF group (except the highest) is a subgroup of another group. The RACF-supplied group SYS1 must be the highest group in the structure. The relationship between superior groups and subgroups is administrative and does not necessarily imply any authorization to resources.

Identifying Your Users

The implementation and use of RACF involves several different types of users:

- Security administrator
- Group administrator
- Auditor
- Operations and technical support person
- Other users

As part of planning for RACF, you need to understand the responsibilities of the various users during the planning stages and installation of RACF. Figure 13 lists typical user responsibilities.

Note: Management has the responsibility for defining security policies and ensuring the security controls are maintained.

User	Responsibility
Security Administrator	The security administrator has the overall responsibility for RACF implementation. The security administrator reviews and approves all implementation phases, selects the resources to be protected, and plans the order in which protection will be implemented. In addition, the security administrator should be responsible (or should delegate the responsibility to group administrators) for educating the installation users about how RACF will be implemented. (That is, will there be a grace period before the new security procedures take effect? Or, how will the implementation of RACF affect the day-to-day responsibilities of each user?)
Group Administrator	During planning, the group administrators are user representatives who represent major application areas.
Other Administrators	Other users might be considered as members of the implementation team if appropriate. For example, a data base administrator might be selected to represent protection for the DB/DC environment, including: ● DB/DC users ● Accessibility to DB/DC subsystems ● Terminal and transaction protection ● Data base protection for batch access
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 audit of security measures.
Technical Support	The system programmer who provides technical support for RACF installs RACF in the system and maintains the RACF data set. This person has overall responsibility for the programming aspects of system protection and provides technical input on the feasibility of various aspects of the implementation plan. In addition, the technical support person writes, installs, and tests RACF exit routines. Note that, while there is no "technical support" attribute, this person has an important role in implementing RACF. The technical support person might very well be assigned the RACF OPERATIONS attribute.
Operations	The user with the OPERATIONS attribute has authority to perform certain "housekeeping" operations on RACF-protected resources (for example, dump/restore).

Figure 13. RACF Users and Their Typical Responsibilities

Chapter 5: RACF Version 1 Release 7

RACF Version 1 Release 7 is a major release that includes all of the functions provided by RACF Version 1 Release 6. RACF also now offers significant new facilities, such as program control, tape data set protection, erase-on-scratch, and security classification checking, as well as other enhancements for increased security, usability, and auditability.

This chapter describes:

- Highlights of RACF Version 1 Release 7
- Hardware and software operating environment, including and migration/coexistence considerations
- Storage estimates for the required virtual storage, system libraries, RACF data set, and ISPF

Version 1 Release 7 Highlights

Following is a brief description of the highlights of RACF Version 1 Release 7. If the enhancement has "MVS only," it applies to both MVS/370 and MVS/XA systems, but not to VM systems. If the enhancement has "MVS/XA only," it does not apply to MVS/370 and VM systems. Each description also has a note, if needed, that contains any other general restrictions on the operating environment. For detailed information on the required PTFs (program temporary fixes), see the RACF Version 1 Release 7 Program Directory.

Program Control (MVS/XA only)

Program control is a RACF option that consists of two parts: access control to load modules, and program access to data sets.

Access control to load modules allows only authorized users to load and/or execute specified load modules (programs) in SYS1.LINKLIB, or other libraries concatenated to SYS1.LINKLIB via the system LINKLIST. RACF uses a new general resource class (PROGRAM) to maintain profiles that represent programs. Each program has an access list that contains userids and/or group names and their access authority. Anyone with READ access authority or higher can execute a controlled program.

Program access to data sets allows an authorized user or group of users to access specified data sets in conjunction with the user's authority to execute a certain program. That is, the user can access specified data sets at a specified access level

while executing a certain program (access to the program itself may be controlled by using access control to load modules).

RACF implements program access to data sets by using another access list, called a conditional access list, in the profiles of resources in the DATASET class. Each entry in the conditional access list consists of a userid or group id, an associated program name, and an access authority (such as READ or WRITE). The user can access the data set at that access level while executing the associated program.

Note: Program control requires MVS/SP Version 2 Release 1.2 or later, and a PTF on the MVS release. Program access to data sets also requires Data Facility Product (DFP) Version 2 Release 1 and a PTF on DFP Version 2 Release 1.

DASD Erase-on-Scratch Support (MVS/XA only)

Installations have the option of causing the physical erasure of security-sensitive data at the time the data set extents are scratched (deleted) or released for reuse. RACF associates an erase-on-scratch indicator with DASD data set profiles. RACF passes the indicator setting to data management during a scratch or partial release operation. If the indicator is on, data management physically erases the data set being deleted.

Note: DASD erase-on-scratch requires DFP Version 2 Release 1 plus a PTF on DFP Version 2 Release 1.

Expanded RACF/CICS Security Support (MVS only)

RACF can provide protection at the command level for all resources previously protected by resource-level security checking. For command level programming, these resources now also include CICS/VS started transactions, files, journals, programs, transient data destinations, and temporary storage definitions. Installations can specify the resource checking by class.

Other enhancements are:

- New resources can be protected by RACF while CICS/VS is running.
- Unsuccessful attempts to access protected resources are logged to SMF.
- Logging of additional data when sign-on fails as well as optional logging of data for successful sign-on/logon and successful sign-off/logoff.
- Utilization of the MVS system authorization facility (SAF) for RACF security support.

Note: To use these enhancements, CICS/OS/VS Version 1 Release 7 (Program Number 5740-XX1) must be installed.

User or Terminal Time/Day-of-Week Control

Installations can control a user's access to the system by limiting the user's ability to logon to certain days of the week, and certain hours within each day. Installations can also limit the use of individual terminals to certain days of the week, and certain hours within each day.

RACF also provides support for installations that have terminals in different time zones. RACF allows the installation to associate with each terminal the terminal's location relative to the local time where the processor complex, on which RACF is executing, is located.

Realtime Violation Notification (MVS only)

RACF provides the option of issuing a message to notify a RACF-defined user of an attempted access by an unauthorized user to a protected resource. (This message is in addition to message ICH408I, which RACF sends to the system console.) Users can specify the user to notify on the ADDSD, ALTDSD, RDEFINE, and RALTER commands.

If the user is not logged on when RACF issues the message, the user receives the message at the next logon.

Note: Realtime violation notification is for TSO users only.

Tape Data Set Protection (MVS/XA only)

Installations can establish data set access requirements based on data set names. RACF also provides protection for unlabeled tapes on a volume basis, by using the volume serial coded on the JCL statement to perform validation.

When tape data set protection is active, RACF maintains profiles in the DATASET class, similar to the profiles for DASD data sets. If the TAPEVOL class is active, RACF also maintains profiles in the TAPEVOL class. RACF links the two profiles by using a tape volume table of contents (TVTOC) that is similar to the VTOC of a direct-access volume. The TVTOC is kept in the RACF data set as part of the tape volume (TAPEVOL) profile.

When RACF TVTOCs are being maintained, RACF allows users to specify a security retention period for tape data sets. RACF uses the security retention period to prevent deleting the data set or overwriting the data set with a data set of a different name.

Note: Tape data set protection requires DFP Version 2 Release 1 plus a PTF on DFP Version 2 Release 1.

Tape Bypass Label (BLP) Processing Control (MVS/XA only)

RACF provides a new general resource class (FACILITY) that it uses when checking authorization to use the BLP (bypass label processing) parameter on JCL statements for tape data sets.

Note: Tape bypass label processing requires DFP Version 2 Release 1 plus a PTF on DFP Version 2 Release 1.

Security Classification of Users and Data

Security classification of users and data is a new function that enables installations to impose additional access controls on sensitive resources. An installation can define categories and security levels for both users and data sets.

A **category** is an installation-defined name corresponding to a department or area within an organization with similar security requirements. For example, all of the people who work on the accounting program could be in a category called *accounting*. The second type of information is a security level. A **security level** is an installation-defined name that corresponds to a numerical security level (the higher the number, the higher the security level). For example, a user might have a security level of *confidential*. The installation has defined the security level of *confidential* to be equal to 150.

When a user requests access to a resource, RACF compares the user's categories and security level with the resource's categories and security level to determine whether the user has an adequate "security classification" for that resource.

Data Security Monitor Enhancements (MVS only)

The data security monitor (DSMON) has several new reports and allows the user to control which functions DSMON performs. The new reports are:

- **Started procedures table report**, which lists, for each procedure in the started procedures table, the procedure name, the userid and group name to be associated with the procedure, and whether the procedure is privileged (all RACHECKs for that procedure are considered successful).

- **Class descriptor table report**, which lists, for each general resource class, the class name, the default UACC, whether the class is active, whether auditing is being done, whether statistics are being kept, and whether OPERATIONS attribute users have access.

- **Global access table report**, which lists, for each general resource class in the global access table, all the entry names and their associated global access checking authority levels.

- **Group tree report**, which lists, for each requested group, all its subgroups, all the subgroups' subgroups, and so on, as well as the owner of each group listed in the report.

The new program control facility can be used to control who is authorized to use DSMON. (Otherwise, only persons with the AUDITOR attribute can execute DSMON.)

Note: The DSMON authorization enhancement requires the RACF program control facility, which requires MVS/SP Version 2 Release 1.2 or later, and a PTF on the MVS release.

RVARY Command Authorization Enhancement

In response to an RVARY command, the operator must enter an installation-defined password in order to approve an activation/deactivation of RACF, or a switching of the RACF data sets. The SETROPTS command allows a SPECIAL user to define separate passwords for RACF activation/deactivation and for switching the RACF data sets.

Data Set Protect-all Option (MVS only)

The protect-all option allows the creation of a new data set only if the data set will be RACF-protected by either a discrete or generic profile.

Control of REVOKE/RESUME by Date

RACF allows the specification of a future date on which RACF revokes or restores a user's authority to access the system. For example, if a person is taking a three-week vacation, the manager (an authorized user) can issue a command today that revokes the userid on the day the person leaves and restores it on the day the person returns.

Class Descriptor Table and RACF Router Table Split

The class descriptor table and RACF router table each consist of two separate load modules. One load module is for IBM-defined classes, the other is for the installation-defined classes. This split simplifies the installation of new RACF releases.

Logging OPERATIONS Authority

An installation has the option of logging all accesses to resources granted because the user has the OPERATIONS or group-OPERATIONS user attribute.

Virtual Storage Constraint Relief (MVS only)

Virtual storage constraint relief for MVS/XA consists of providing support for callers and parameters above 16 megabytes and relocation of certain RACF data areas above 16 megabytes Both of these items will contribute to a savings of virtual storage below 16 megabytes.

Additionally, for both MVS/370 and MVS/XA, certain ACEE-related control blocks are eliminated for multiple-user address spaces, such as IMS/VS and CICS/VS. This reduces the amount of storage required for the RACF control blocks related to sign-on.

Enhanced support for RACF ISPF Panels (MVS only)

The RACF listing command processors (LISTDSD, LISTGRP, LISTUSER, RLIST and SETROPTS LIST) enable users to browse (scroll) the output.

Note: To use the RACF ISPF (Interactive System Productivity Facility) panels, ISPF Version 1 or Version 2, and TSO Extensions (TSO/E) Release 2 or later (or an equivalent) must be installed.

LISTDSD and RLIST Enhancements

These commands display the true access authority, from any source, that a user has to a resource. This access authority appears under the heading YOUR ACCESS in the LISTDSD and RLIST output. The user's access authority could be from global access checking, the OPERATIONS attribute, the universal access authority for the resource, and so forth.

ADDSD and RDEFINE Modeling Enhancements

New operands on these commands enable the user to copy information from an existing profile to a new profile.

RACINIT Without Generating Statistics

The caller of RACINIT can suppress statistics when multiple RACINIT invocations occur for a single situation.

SYSGEN No Longer Required to Install RACF (MVS/XA only)

An installation can install RACF without a stage-1 system generation because RACF installs its own SVC routines.

Operating Environment

This section contains the software and hardware requirements, as well as some migration/coexistence considerations for RACF Version 1 Release 7.

Software

RACF Version 1 Release 7 can be used with MVS/System Product Version 1 Release 3 and later, or MVS/System Product Version 2. However, some of the new RACF functions require programming support that may not be available in all of these releases of MVS. (See the individual descriptions under "Version 1 Release 7 Highlights" in the preceding section.) In these cases, while RACF will be available, some of its functions will not be.

RACF Version 1 Release 7 can also be used with VM/System Product Release 3 or later, with or without the High Performance Option Release 3.2 or later, when used in conjunction with the RACF/VM Support PRPQ (IBM Program Number 5767-002). However, certain functions of RACF Version 1 Release 7 are not effective. These functions are available and can be used, but they have no effect on the security processing done on VM. (See "Version 1 Release 7 Highlights" for functions that are MVS only or MVS/XA only.) However, in a shared VM-MVS environment, the sharing MVS system can still use these functions.

To assemble the RACF optional source materials, Assembler H Version 2 (IBM Program Number 5668-962) must be installed.

If the RACF report writer is used, DFSORT (IBM Program Number 5740-SM1) or an equivalent must be installed.

RACF is supported by TSO and TSO/E in a ACF/TCAM or ACF/VTAM environment.

To use the RACF ISPF (Interactive System Productivity Facility) panels, ISPF Version 1 (IBM Program Number 5668-960) or Version 2 (IBM Program Number 5665-319) must be installed. TSO Extensions (TSO/E) Release 2 or later (IBM Program Number 5665-285), or an equivalent, must also be installed.

JES2 and JES3 Version 1 Release 3.4 and later (plus a PTF), and JES2 and JES3 Version 2 Release 1.2 and later (plus a PTF) facilitate batch job identification. These releases support the propagation of RACF-validated userids to the batch job initiator.

TSO Extensions (TSO/E) or the MVS TSO Command Package (or equivalent) must be installed if the installation wishes to use SUBMIT command operands to facilitate the submission of batch jobs that access RACF-protected resources.

To use RACF for IMS/VS user identification and transaction authorization, IMS/VS Version 1 Release 1.5 or later (IBM Program Number 5740-XX2) must be installed.

To use RACF for CICS/VS user identification and transaction authorization, CICS/OS/VS Version 1 Release 5 or later (IBM Program Number 5740-XX1) must be installed. To use RACF to protect CICS/VS resources other than transactions, CICS/OS/VS Version 1 Release 7 must be installed.

If the installation uses Data Facility Hierarchical Storage Manager (DFHSM) and plans to use the RACF generation data group (GDG) modeling and/or the naming conventions installation exit, then HSM Release 3 or later (IBM Program Number 5740-XRB) must be installed.

HSM Release 3 and Release 3.1 do not support always-call. If the generic profile facilities are elected for use with these HSM offerings, these facilities will not be protected for the execution of the HSM functions.

Hardware

RACF Version 1 Release 7 is designed to operate on the IBM processors supported by MVS/System Product Version 1 Release 3 and later, MVS/System Product Version 2, and VM/System Product Release 3 or later.

On an MVS system, RACF has no special hardware requirements in addition to those normally required by these products. On a VM system, the RACF data base must reside on a 3330, 3350, 3375, or 3380 DASD (direct access storage device).

For TSO operator identification card (OIDCARD) support, RACF Version 1 Release 7 can be used with the following subset of IBM devices supported by TSO:

- Operator identification card reader on the IBM 3270 Information Display System (SNA and non-SNA devices)

- ID reader on the IBM
  - 3771 Communication Terminal (Models 1, 2, and 3)
  - 3773 Communication Terminal (Models 1, 2, and 3)
  - 3774 Communication Terminal (Models 1 and 2)
  - 3775 Communication Terminal (Model 1)
- Magnetic stripe reader on the IBM 3767 Communication Terminal (SNA devices only)
- Magnetic slot reader and magnetic hand scanner on a 3278 or 3279 terminal attached to a 3274 control unit with the 10/63 alphanumeric character set

On an MVS system, you can have an optional dedicated security console. RACF routes messages to this console for detected unauthorized access attempts. The console may be any console supported by MVS.

The volume of logging (SMF) data generated by RACF depends on the various RACF logging options selected by the installation, the number of protected resources for which logging is selected, and the frequency of accessing these resources. The installation should review the volume of logging data to determine the possible need for increasing the size of the SMF data set(s).

Migration/Coexistence Considerations

RACF Version 1 Release 7 is designed so that an installation can easily migrate to it from Version 1 Release 6 by executing the RACF Data Set Initialization Utility Program (ICHMIN00) to convert the templates in the RACF data set. Following the conversion, you can use the two releases of RACF concurrently or alternately, because either release of RACF will function properly with the converted RACF data set.

However the enhanced capabilities of RACF Version 1 Release 7 do create a few migration considerations.

Consider the following items when RACF Version 1 Release 6 and Version 1 Release 7 are to be used concurrently on systems that share resources, or alternately during a migration period:

- The tape data set protection option is not available in RACF Version 1 Release 6, but, when a tape data set is protected with Version 1 Release 7, the tape volume will also be protected as in Version 1 Release 6. However, on systems sharing the RACF data set, do not issue data set profile commands (ADDSD, ALTDSD, and DELDSD) from the RACF Version 1 Release 6 system for profiles created by the tape data set protection option. Also, you should not issue a RACDEF-DELETE to delete a TAPEVOL (or DATASET) profile without also deleting the corresponding DATASET (or TAPEVOL) profile. Each installation will need to consider the possible conflicts that might occur.

- In environments that have different releases of RACF being used concurrently, the WHEN(PROGRAM) operand is invalid for (ignored by) any RACF release prior to Version 1 Release 7. Also, the program control option is valid only on an MVS/XA system. Using the program control operands in other environments causes RACF to ignore them and issue an error message.

Other migration considerations might be:

- TSO IKJPARSE routines allow a user to abbreviate an operand on a TSO command to the least number of characters that cause that operand to be distinguished from all other operands.

  With the addition of many operands to the RACF command in Version 1 Release 7, it is possible that some conflicts in abbreviations may occur. For example, with RACF Version 1 Release 6, you could abbreviate LIST on the SEARCH command as L. However, with Version 1 Release 7, the new LEVEL operand on the SEARCH command makes the abbreviation L ambiguous. You could use LI for LIST to distinguish it from LEVEL. It is strongly recommended that you fully spell-out all operands on commands that are hard coded (for example, in programs, CLISTs, and EXECs). In an interactive environment, abbreviations are acceptable because the parse routines prompt the user when any conflicts occur.

- A TVTOC should not be maintained for HSM tapes, because there are many data sets on the same tape, and the RACF tape data set profile will become very large. Therefore, it is strongly recommend that installations with HSM and RACF tape data set support active issue the command RALTER TAPEVOL HSMHSM NOTVTOC to avoid any problems.

- If you already have an installation-defined class for programs, you can use the RDEFINE command with the FROM operand to "copy" the profile information into the PROGRAM general resource class.

- If you do not follow the rules for defining your own general resource classes, RACF Version 1 Release 7 issues warning MNOTEs when you assemble the optional, installation-supplied class descriptor table. RACF issues an MNOTE if the class name does not contain a national character or number in one of the first four positions, the ID value is not in the range of 128-255, or the POSIT value is not in the range of 25-31.

- The new class descriptor table entries are:

  - FACILITY (bypass label processing)
  - SCDMBR (security classification of users and data member)
  - SECDATA (for security classification of users and data)
  - FCICSFCT (file control table)
  - HCICSFCT (file control table group)
  - JCICSJCT (journal control table)
  - KCICSJCT (journal control table group)
  - DCICSDCT (destination control table)
  - ECICSDCT (destination control table group)
  - SCICSTST (temporary storage table)
  - UCICSTST (temporary storage table group)

- MCICSPPT (processing program table)
- NCICSPPT (processing program table group)
- ACICSPCT (program control table)
- BCICSPCT (program control table group)
- PMBR (program member)
- PROGRAM (for programs)

- The following subsystem (SUBSYS) and requestor (REQSTOR) names are added to the IBM-supplied RACF router table for use by the tape data set and program control functions:

  - REQSTOR=PROGMCHK,SUBSYS=CONTENTS
  - REQSTOR=CLOSE,SUBSYS=OCEOV
  - REQSTOR=TAPEOPEN,SUBSYS=OCEOV
  - REQSTOR=TAPERST,SUBSYS=RESTART

- Installations that are migrating from a system without always-call support to a system with always-call support should be aware that always-call systems protect VSAM data sets based only on the cluster name. With always-call, it is no longer necessary to protect the index and data components, as well as the VSAM cluster itself. In addition, with always-call, the index and data components will not have RACF profiles automatically built for them because of ADSP or the PROTECT operand on the access method services (IDCAMS) DEFINE command. Also, the IDCAMS DELETE command does not delete RACF profiles for index and data components.

  Because of the VSAM-protection implementation differences between systems with always-call and without always-call, use caution if you are sharing the RACF data set between a system with always-call and a system without always-call. In multi-system environments, it is recommended that you use compatible levels of Data Facility Product (DFP).

Storage Estimates

Use the following information to assess your storage requirements for virtual storage, system libraries, the RACF data set, and ISPF.

Virtual Storage Requirements:

The approximate virtual storage requirements for RACF Version 1 Release 7 are:

Area	Bytes for RACF Version 1 Release 7
FLPA	8000 bytes minimum. See Note 1.
PLPA	205,000 bytes minimum. See Note 1.
SQA	1300 bytes minimum. See Note 2.
LSQA	4200 bytes (5200 bytes if RACF data set is on a shared device). See Note 3. Variable if RACLIST or generic profiles are used. See Note 4. Variable for multiple-user address spaces. See Note 5.
CSA	Variable. See Note 6 and Note 7.
Private Area	8200 bytes -- fetch protected. See Note 3.

Notes:

1. If RACF is used for IMS/CICS authorization checking, the FRACHECK service routine and the IMS/VS-to-RACF routines must be in fixed LPA to ensure good performance. If RACF is not used for IMS/CICS authorization checking, you can place these modules in pageable LPA and add the estimates for FLPA to those for PLPA.

   If an installation exit routine is provided for the FRACHECK service routine, it should be in the same virtual storage area as the FRACHECK service routine. Add the size of this routine to FLPA or PLPA accordingly. Also included in the PLPA are any installation-written exit routines and the started procedures replaceable module that you have included in the system. Add the size of these modules to the PLPA requirement.

2. The IBM-supplied class descriptor table and RACF router table require approximately 800 bytes. Add the size of your installation-defined class descriptor table and RACF router table to the SQA requirement.

3. These LSQA and private area figures apply to each address space while it is executing a RACF function. However, every address space must have 164 bytes of LSQA at all times.

   On an MVS/XA system, the LSQA requirement for CICS/VS can be minimized with the use of CICS/OS/VS Version 1 Release 7.

4. For the RACLIST function, the amount of LSQA storage needed depends on variables such as, the number of resident generic profiles, the number of resources in a given class, and the length of installation and/or application data for these resources.

   If generic profiles are used, the amount of LSQA storage required also depends on the number of classes and data set high-level qualifiers referenced and the number of generic profiles associated with each.

5. For multiple-user address spaces, such as IMS/VS and CICS/VS, an additional amount must be added for each user. The amount for each user depends on variables such as: whether list-of-groups checking is active, the number of groups the user is connected to, and whether the user's RACF profile has installation data.

   The issuer of RACINIT can cause this storage to be allocated outside of LSQA by specifying the subpool parameter.

6. There are two formulas for CSA: one if fetch-protected and the other if not fetch-protected.

   If not fetch-protected, the formula is based on the number of resident index/data blocks and the number of primary RACF data sets. The IBM supplied default is 15,400 bytes.

   If fetch-protected, the formula depends on the number of references to RACF-protected VSAM catalogs by VSAM catalog-management routines. The storage required for each catalog is 70 bytes plus 9 times the number of

users and groups in the access list for the data set profile of the RACF-protected VSAM catalog.

7. On an MVS/XA system, the CSA requirement is reduced by moving the in-storage buffers above 16 megabytes. The savings for each installation will vary depending upon the installation. But, as a general estimate, an installation with 40 buffers can expect to save about 40,000 bytes.

The RACF commands require only a TSO address space.

See *System Programming Library: RACF* for more detailed information.

System Library Storage Requirements:

The approximate space requirements for the system libraries (based on the IBM 3350 Disk Storage and a track size of 19,069 bytes) for RACF Version 1 Release 7 are:

Library	Tracks for RACF Version 1 Release 7
SYS1.LINKLIB	100
SYS1.LPALIB	20-22
SYS1.MACLIB	21
SYS1.HELP	10
SYS1.SAMPLIB	1

Note: Add the required tracks for any installation-written exit routines installed for RACF.

RACF Data Set Storage Requirement:

RACF requires the allocation of a non-VSAM data set on direct access storage for all RACF access control information. The RACF data set should be on a permanently resident volume and, if the RACF data set is to be shared between systems that have RACF installed, the volume must be on a shared DASD (direct access storage device).

The direct access space needed for the RACF data set depends mainly on the number of users, groups, user-group connections, and resources profiles defined to RACF. The size also depends on the name lengths of the entities defined to RACF and how efficiently the space within the RACF data set is utilized. On the average, a RACF data set requires approximately 320K bytes for each 1000 entities defined to RACF.

Interactive System Productivity Facility (ISPF) Requirements:

The approximate space requirements for the ISPF data sets (based on the IBM 3350 Disk Storage and a track size of 19,069 bytes) for RACF Version 1 Release 7 are:

ISPF DD Name	Tracks for RACF Version 1 Release 7
ISPPLIB	85
ISPSLIB	17
ISPMLIB	7
SYSPROC	2

Appendix A: RACF Command Functions

RACF commands allow you to add, modify, list, and delete profiles for users, groups, connect entries, and resources. This appendix (Figure 14) shows, in alphabetic order, each of the commands and lists the functions. Appendix B (Figure 15) shows the attributes and authorities required to issue each command.

RACF Command	Command Functions
ADDGROUP	– Define one or more new groups as a subgroup of an existing group. – Specify a model data set profile for a group.
ADDSD*	– RACF-protect one or more existing data sets. – RACF-define one or more data sets brought from another system where they were RACF-protected. – RACF-define generic DATASET profiles. – Create a new data set model profile.
ADDUSER	– Define one or more new users and connect the users to their default connect group. – Specify a model data set profile for a user.
ALTDSD*	– Change one or more discrete or generic DATASET profiles. – Protect a single volume of a multivolume, non-VSAM DASD data set. – Remove protection from a single volume of a multivolume, non-VSAM DASD data set.
ALTGROUP	– Change the information in one or more group profiles (such as the superior group, owner, or model profile name).
ALTUSER*	– Change the information in one or more user profiles (such as the owner, universal access authority, or security level). – Revoke or re-establish one or more users' privileges to access the system. – Specify logging of information about the user, such as the commands the user issues.
CONNECT	– Connect one or more users to a group. – Modify one or more users' connection to a group. – Revoke or re-establish one or more users' privileges to access the system.
DELDSD*	– Delete one or more discrete or generic DATASET profiles. – Delete a discrete DATASET profile for a tape data set, while retaining the data set name in the TVTOC. – Remove a data set profile, but leave the data set RACF-indicated, when moving a RACF-protected data set to another system that has RACF.
DELGROUP*	– Delete one or more groups and their relationship to the superior group.
DELUSER*	– Delete one or more users and remove all their connections to RACF groups.
LISTDSD*	– List the details of one or more discrete or generic DATASET profiles, including the users and groups authorized to access the data set(s).
LISTGRP	– List the details of one or more group profiles, including the users connected to the group.
LISTUSER	– List the details of one or more user profiles, including all the groups each user is connected to.
PASSWORD*	– Change one or more users' passwords. – Change one or more users' password change interval. – Reset one or more users' passwords to a known default value.
*Installation exit point provided.	

Figure 14 (Part 1 of 2). Functions of RACF Commands

RACF Command	Command Functions
PERMIT*	– Give or remove authority to access a resource to specific users or groups. – Change the level of access authority to a resource for specific users or groups. – Copy the list of authorized users from one resource profile to another. – Delete an existing standard access list. – Maintain a conditional access list.
RALTER*	– Change the discrete and/or generic profiles for one or more resources whose class is defined in the class descriptor table. – Maintain the global access checking tables. – Maintain category and security level tables.
RDEFINE*	– RACF-protect by a discrete and/or generic profile one or more resources whose class is defined in the class descriptor table. – Define the global access checking tables. – Define category and security level tables.
RDELETE*	– Remove RACF-protection from one or more resources whose class is defined in the class descriptor table. – Delete the global access checking tables. – Delete the category and security level tables.
REMOVE*	– Remove one or more users from a group and assign a new owner for any group data sets owned by the users.
RLIST*	– List the details of discrete and/or generic profiles for one or more resources whose class is defined in the class descriptor table.
RVARY	– Dynamically deactivate and reactivate the RACF function. – Dynamically deactivate and reactivate the RACF backup data set. – Switch the primary and back-up RACF data sets. – Deactivate resource protection, for any resource whose class is defined in the class descriptor table, while RACF is deactivated.
SEARCH*	– List the RACF profile names that meet a search criteria for a class of resources. – Create a CLIST of the RACF profile names that meet a search criteria for a class of resources.
SETROPTS	Dynamically set system-wide options relating to resource protection, specifically: – Choose the resource classes defined in the class descriptor table that RACF is to protect. – Gather and display RACF statistics. – Set the universal access authority (UACC) for terminals. – Specify logging of certain RACF commands and events. – Permit list-of-groups access checking. – Control the use of automatic data set protection (ADSP). – Activate profile modeling for GDG, group, and user data sets. – Enable or disable generic profile checking on either a class-by-class or system-wide level. – Control user password syntax rules. – Establish password syntax rules. – Activate password processing for checking previous passwords, limit invalid password attempts, and warn of password expiration. – Control global access checking for selected individual resources and/or generic names with selected generalized access rules. – Activate protection for data sets with single-level names. – Control logging of real data set names. – Control the job entry subsystem (JES) options. – Initiate refreshing of in-storage generic profile lists and global access checking tables. – Activate tape data set protection. – Select a security retention period for tape data sets. – Control whether or not new data sets must be RACF-protected. – Control the erasure of scratched DASD data sets. – Activate program control. – Set the passwords for authorizing use of the RVARY command. – Activate security classification of users and data. – Display the current options.
*Installation exit point provided.	

Figure 14 (Part 2 of 2). Functions of RACF Commands

Appendix B. RACF Commands, Authorities, and Attributes

The following chart summarizes the authorities and attributes required to issue each RACF command. See the *RACF Command Language Reference* for a complete description of each command and the user requirements.

RACF Command	Required Authority 1	*Owner of:*			*Group-Related Authorities/Attributes 2*							*User Attribute 3*				*Access Authority*			
		User	Group	Resource 4	JOIN	CONNECT	CREATE	USE	SPECIAL	OPERATIONS	AUDITOR 5	SPECIAL 6	OPERATIONS	AUDITOR 5	CLAUTH	ALTER 7	CONTROL	UPDATE	READ
ADDSD	8				X	X	X		9	10		X	10						
ADDGROUP	11		X		X				X			X							
ADDUSER	12		X		X				X			X			X				
ALTDSD				X					X		X	X		X		X			
ALTGROUP			X		X				X			X							
ALTUSER	13	X	X		X	X			X		X	X		X					
CONNECT			X		X	X			X			X							
DELDSD				X					X			X				X			
DELGROUP			X		X				X			X							
DELUSER		X							X			X							
LISTDSD				X					X	X	X	X	X	X		X	X	X	X
LISTGRP			X		X	X			X	X	X	X	X	X					
LISTUSER	14	X							X	X	X	X	X	X					
PASSWORD	15	X							X			X							
PERMIT				X					X			X				X			
RALTER				X					X		X	X		X		X			
RDEFINE												X			X				
RDELETE				X					X			X				X			
REMOVE				X	X	X			X			X							
RLIST			X						X	X		X	X	X		X	X	X	X
RVARY	16																		
SEARCH				X					X	X	X	X	X	X		X	X	X	X
SETROPTS									17	17	17	X	17	X	17				

Figure 15. Authorities Required to Issue RACF Commands

Notes:

1. To issue a RACF command, the user must be defined to RACF and have sufficient authority as shown in the body of this table. In some cases, additional authority is required to use some command options. See the *RACF Command Language Reference* for full details.

2. Group authorities and attributes are assigned via the CONNECT command. They are effective only when dealing with data sets and profiles related to the group in which the user was assigned the authority.

   The JOIN, CONNECT, CREATE and USE authorities are effective only in the group for which they were assigned.

   The group-SPECIAL, group-OPERATIONS, and group-AUDITOR attributes are effective in the group in which they were assigned, all subgroups owned by the group, subgroups owned by these subgroups, and so on. These attributes percolate down through the group tree structure.

   A user with the group-SPECIAL, group-OPERATIONS, or group-AUDITOR attribute in a group is authorized to the profile for:

   - The group
   - Subgroups owned by the group
   - Users owned by the group
   - Data sets owned by the group
   - Data sets with a high-level qualifier that is name of the group or a subgroup owned by the group.
   - Data sets owned by users who are owned by the group
   - Data sets with a high-level qualifier that is a userid owned by the group or a subgroup owned by the group.
   - General resources owned by the group or a subgroup owned by the group.
   - General resources owned by users who are owned by the group or by a subgroup that is owned by the group.

3. User attributes are assigned via the ADDUSER and ALTUSER commands and give the user system-wide authority. These attributes are not restricted to use on specific profiles.

4. For data sets, a user is also considered to be the owner of a profile if the high-level qualifier of the profile name is the user's userid. If the owner of the profile is a group, then a user with the group-SPECIAL or group-AUDITOR attribute in the group is authorized to modify the profile.

5. A user with the AUDITOR or group-AUDITOR attribute is restricted to setting auditing (logging) options and to listing functions.

6. A user with the SPECIAL attribute is authorized to issue all commands for all profiles, with the exception of those options that are restricted to users with the AUDITOR attribute.

7. ALTER authority is normally required to modify a profile and to list the profile's access list. For generic profiles, the user must be authorized by ownership or user or group attributes.

8. A user can create data set profiles if the high-level qualifier is the user's own userid or a group name in which the user has at least CREATE authority.

9. A group-SPECIAL user can create data set profiles if the high-level qualifier is a group in which the user is group-SPECIAL or a userid owned by a group in which the user is group-SPECIAL.

10. An OPERATIONS user can create data set profiles if the high-level qualifier is a group name and the user is not connected to that group with less than CREATE authority.

    A group-OPERATIONS user can create data set profiles if the high-level qualifier is a group in which the user has group-OPERATIONS.

11. The user must be the owner of the superior group, or be connected to the superior group with JOIN authority or the group-SPECIAL attribute.

12. The user must have class authority in the USER class and (a) be the owner of the default group, or (b) be connected to the default group with JOIN authority or the group-SPECIAL attribute.

13. All users can modify their own name fields and default groups.

14. All users can list their own user profiles.

15. All users can set their own password and password interval, subject to their installation's guidelines.

16. The operator (at the master console or security console) must approve the request by entering an installation-defined password.

17. Only users with the SPECIAL or AUDITOR attribute can change system options.

Glossary

(See also the *Vocabulary for Data Processing, Telecommunications, and Office Systems*, GC20-1699)

access. The manner in which files or data sets are referred to by the computer. In RACF, the ability to obtain the use of a protected resource.

access authority. An authority that relates to a request for a type of access to protected resources. The access authorities are NONE, READ access, UPDATE access, CONTROL access (for VSAM data sets), and ALTER access.

accessor environment element (ACEE). A description of the current user including userid, current connect group, user attributes, group authorities. An ACEE is constructed during user identification and verification.

access control to load modules. A RACF function that allows only authorized users to load and/or execute specified load modules.

access list. A list within a profile of all authorized users and their access authorities.

ACEE. See accessor environment element.

alphanumeric. The set of characters that includes alphabetic (A through Z), numeric (0 through 9), and national (#, $, and @) characters.

always-call. A data management function that calls RACF whenever a data set is accessed (whether the data set is RACF-indicated or not) or DASD space is allocated for a data set.

automatic data set protection (ADSP). A user attribute that causes all permanent data sets created by the user to be automatically defined to RACF.

automatic profile. A TAPEVOL profile that RACF creates when a RACF-defined user protects a tape data set. The TAPEVOL profile created in this manner is called an automatic profile because, when RACF deletes the last data set on the volume, RACF automatically deletes the TAPEVOL profile. Also see non-automatic profile.

attribute. See user attribute.

authority. The ability to perform a function on a RACF-defined user, group, or resource. See access authority, group authority, class authority.

authorization checking. The action of determining if a user is permitted access to a RACF-protected resource.

category. An installation-defined name corresponding to a department or area within an organization with similar security requirements.

class. A collection of RACF-defined entities with similar characteristics.

class authority. An authority that allows a user to define entities to RACF in the classes defined in the class descriptor table.

class descriptor. RACF-supplied control block for all the resource classes in the class descriptor table (which is all the classes except the USER, GROUP, and DATASET classes).

class descriptor table. A table consisting of an entry for each class except the USER, GROUP, and DATASET classes. The table is generated by specifying the ICHERCDE macro once for each class.

class name. The name that identifies a RACF class of entities. The class names are USER, GROUP, DATASET, and those class names found in the class descriptor table.

conditional access list. An second access list within a resource profile that associates a program name with each userid and the corresponding access authority. The user can access the data set at the specified access authority while executing the associated program. See also access list.

connect profile. A description of a RACF-defined user's relationship to a group, including group authority and group-related user attributes.

current connect group. The group with which a user is associated during a terminal session or batch job.

data security. The protection of data from unauthorized disclosure, modification, or destruction, whether accidental or intentional.

data security monitor (DSMON). A RACF auditing tool that produces reports that enable an installation to verify its basic system integrity and data security controls.

data set profile. A description of a RACF-defined data set, including data set name, owner, volume serial number, universal access authority, security level, and other data.

default group. The group with which a user is associated when a group name is not specified on the TSO LOGON command or batch JOB statement. (On a VM system, you cannot specify a group name.)

delegation. The act of giving other users or groups authorities to perform RACF operations.

discrete profile. A description of a single RACF-defined resource that belongs either to the DATASET class or to one of the general resource classes. This description includes the authorized users, the access authority of each user, the location of the data set (device type and volume serial number), the number of accesses to the data set, and other information.

entity. A user, group, or resource (for example, a DASD data set or a tape volume) that is defined to RACF.

erase-on-scratch. The physical overwriting of data on a DASD data set when the data set is deleted (scratched).

generation data group (GDG). A collection of data sets with the same base name, such as PAYROLL, that are kept in chronological order. Each data set is called a generation data set.

generic profile. A description of one or more RACF-protected resources that belong either to the DATASET class or to one of the general resource classes and have similar names and similar access-authorization requirements. This description includes the authorized users, the access authority of each user, and other information.

global access checking. The ability to allow an installation to establish an in-storage table of default values for authorization levels for selected resources. RACF refers to this table prior to performing normal RACHECK processing, and grants the request without performing a RACHECK if the requested access authority does not exceed the global value. Global access checking can grant the user access to the resource, but it cannot deny access.

group. A collection of RACF users who can share access authorities for protected resources.

group authority. An authority that relates to a type of function a user can perform in a group. The group authorities are USE, CREATE, CONNECT, and JOIN.

group data set. A data set defined to RACF where either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF group name.

group id. One to eight alphanumeric characters, beginning with an alphabetic, #, $, or @ character, that identifies a group to RACF.

group profile. A description of a RACF-defined group, including group name, superior group name, owner, and users in the group.

group-related user attribute. A user attribute assigned at the group level that allows the user to control the resource, group, and user profiles associated with the group and its subgroups. Some of the group-related user attributes are group-SPECIAL, group-AUDITOR, and group-OPERATIONS.

group terminal option. Users within a group are allowed to LOGON to TSO only from those terminals to which they have been specifically authorized access by the owner of the group.

list-of-groups checking. The function of allowing a user to access all resources available to all groups of which the user is a member, regardless of the specified group to which the user is logged on.

logging. The recording of data about specific events.

modeling. The ability for a user or an installation to define a sample "model" profile that RACF uses when defining a new profile. Each profile model can contain defaults for fields such as the universal access authority, level, owner, auditing flags, access list, erase indicator, security classification information, and installation-defined data.

MVS. Implies both MVS/370 and MVS/XA.

non-automatic profile. A TAPEVOL profile that RACF creates in response to an RDEFINE command or when tape data set protection is not active. A TAPEVOL profile created in this manner is called a non-automatic profile because RACF never deletes the profile except in response to the RDELETE command. Also see automatic profile.

operator identification card (OIDCARD).. A small card with a magnetic stripe encoded with unique characters and used to verify the identity of a terminal operator.

owner. The user or group who creates a profile (or is named the owner of a profile). The owner can modify, list, or delete the profile.

password. A one to eight alphanumeric character string that a user specifies to meet security requirements when entering the system or accessing protected data sets.

profile. A description of the characteristics of a RACF-defined entity. A profile resides on the RACF data set. Also see connect profile, data set profile, group profile, and user profile.

profile list. A list of profiles indexed by class (for general resources) or by the high-level qualifier (for DATASET profiles) and built in storage by the RACF routines.

program access to data sets. A RACF function that allows an authorized user or group of users to access specified data sets in conjunction with the user's authority to execute a certain program. That is, the user can access specified data sets at a specified level while executing a certain program.

program control. Program control is a RACF option that consists of two parts: access control to load modules, and program access to data sets. See also access control to load modules and program access to data sets.

protected resource. A resource that is defined to RACF for the purpose of controlling access to the resource. Some of the resources that can be protected by RACF include DASD and tape data sets, DASD volumes, tape volumes, terminals, IMS/VS transactions, IMS/VS transaction groups, and any other resources defined in the class descriptor table.

RACF. Resource Access Control Facility.

RACF report writer. A RACF function that prints out RACF SMF records and produces reports on system use and resource use from information found in the RACF SMF records.

resource. A facility of the computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs.

Resource Access Control Facility (RACF). A program product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, and logging detected unauthorized attempts to enter the system and detected accesses to protected resources.

security. See data security.

security level. An installation-defined name that corresponds to an numerical security level (the higher the number, the higher the security level).

standard access list. See access list.

TVTOC. The tape volume table of contents (TVTOC) is information about a tape data set that RACF stores in the TAPEVOL profile for the volume on which the data set resides. The TVTOC includes the data set name, data set sequence number, creation date, and an indicator as to whether a discrete tape data set profile exists.

universal access authority (UACC).. The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities.

user. A person who requires the services of a computing system.

user attribute. A characteristic of a user that defines the type of functions the user can perform on entities. The user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE.

user data set. A data set defined to RACF where either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF userid.

user identification. See userid.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the system during TSO logon or batch job processing. RACF identifies the user by the userid and verifies the user by the password and/or operator identification card supplied during TSO LOGON command processing or the password supplied on a batch JOB statement.

user name. One to twenty alphanumeric characters that represent a RACF user.

user profile. A description of a RACF-defined user including the userid, user name, default group name, password, owner, access authority, attributes, security level.

userid. A code that uniquely identifies a user to the system. A userid is one to eight alphanumeric characters beginning with an alphabetic, #, $, or @ character. (Note: On TSO, userids can only be seven characters.)

verification. See user identification and verification.

volume set. The collection of volumes on which a multivolume data set resides. A volume set is represented in one RACF profile.

Index

Resource Access
Control Facility
(RACF)
General Information
Manual

GC28-0722-9

READER'S
COMMENT
FORM

This manual is part of a library that serves as a reference source for systems analysts, programmers, and operators of IBM systems. You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note: ***Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.***

Possible topics for comment are:

Clarity Accuracy Completeness Organization Coding Retrieval Legibility

If you wish a reply, give your name, company, mailing address, and date:

_____

_____

_____

_____

Note: Staples can cause problems with automated mail sorting equipment. Please use pressure sensitive or other gummed tape to seal this form.

Cut or Fold Along Line

What is your occupation? _____

How do you use this publication? _____

Number of latest Newsletter associated with this publication: _____

Thank you for your cooperation. No postage stamp necessary if mailed in the U.S.A. (Elsewhere, an IBM office or representative will be happy to forward your comments or you may mail directly to the address in the Edition Notice on the back of the title page.)

Resource Access Control Facility (RACF) General Information Manual

GC28-0722-9 S370-20

Reader's Comment Form

Cut or Fold Along Line

Fold and tape Please Do Not Staple Fold and tape

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 40 ARMONK, N.Y.

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department D58, Building 921-2
PO Box 390
Poughkeepsie, New York 12602

Fold and tape Please Do Not Staple Fold and tape

Printed in U.S.A.

IBM®

Resource Access Control Facility (RACF) General Information Manual

GC28-0722-9

S370-20

Printed in U.S.A.

IBM®

GC28-0722-09