Global Information Assurance Certification Paper

Jeromy R. Denton

An Introduction to Security Features in Security Server (RACF)

Introduction

Since the earliest days of mainframes, organizations have used IBM's RACF security system to manage security within their operating systems. RACF has since grown beyond the mainframe environment, and provides system-wide security for organizations. Despite the widespread use of this application, many security professionals find themselves securing or auditing a RACF system with little (or no) prior knowledge of RACF. This guide serves as an introduction to help readers gain knowledge about the RACF security system and will discuss some of the essential security features used in RACF.

What is RACF and What Does It Do?

IBM developed a security application, RACF (Resource Access Control Facility), in 1976 to allow companies to secure their organization's information. It originally provided for user authentication, access to data authorization, and journaling. IBM has continually updated and upgraded RACF throughout the years to include many more functions such as easier-to-use interfaces, dynamic options setting, DES password encryption, as well as a host of other controls. In March 1996, the RACF application was integrated into the OS/390 Security Server product, which encompasses a wide array of security components, designed to provide enterprise security. This introduction focuses specifically on the security features included in RACF. (IBM RACF Website)

RACF helps to secure an organization's information environment by providing:

- Flexible control of access to protected resources
- Protection of installation-defined resources
- Ability to store information for other products
- Choice of centralized or decentralized control of profiles
- An ISPF panel interface
- Transparency to end users
- Exits for installation-written routines.

("Security Server (RACF) Introduction")

This discussion focuses on the first two items on the list: access to protected resources using user IDs, their attributes and group profiles, as well as protection of defined resources using data sets and resource profiles. A typical RACF protected system is organized in a certain manner. Users that need access to the same resources are gathered together and placed into groups. These groups are then given access to the data and resources needed by its members. While no means

comprehensive, this introduction provides a first-step in beginning to understand these important security features used in the operation of RACF and will follow this pattern:

1. Several **Users**
2. Are placed into **Groups**
3. Which are given access to **Resources**.

User IDs and Their Attributes

To gain an understanding of the use of ID attributes within RACF, the first step is to understand the user IDs and user profiles used in RACF. To identify and authenticate users, RACF uses a standard user ID and password. Used in combination, this allows RACF to ensure users are who they claim to be. RACF can be set to force many of the current "best practices" in regards to password security. Some of the available options include time between password changes, saving of previous passwords, revoking a user ID after a certain number of unsuccessful login attempts, password syntax rules, and automatically revoking inactive user IDs. (Kimble) This user ID is stored with other information about the user in a group of data called a user profile, which is stored in the RACF database. The profile is what RACF uses to determine if users are allowed on the system and what they can and can not do while using the system. The user profile contains the ID attributes and any groups the user is connected to. ("Security Server (RACF) Introduction") See the section on *Group Profiles* below for more information about groups and connecting users to them.

These password security controls can be reviewed from the SETROPTS report under "Password Processing Options" and "Inactive User-IDs." (Kimble) It is a good practice to ensure that these password options adhere to the organization's password protection policies.

ID attributes define the responsibilities, authorities, or restrictions that a specific user has while defined to the system. ("Security Server (RACF) Introduction") ID attributes can be used at the system or group level. The following discussion relates to attributes at the system level, those attributes that affect a user's authorizations across the entire system, and finishes with group level attributes, those attributes that only affect authorizations within a certain group. See *Group Profiles* below for more information about groups.

The most important, from a security standpoint, system-wide ID attributes that can be included in a user profile are Special, Operations, and Auditor. The Special ID attribute gives the user system-wide access and the ability to create, alter, and delete profiles within the RACF Database. (Winter) This is the most powerful attribute. It allows users to affect the profiles used in RACF, thereby affecting the access granted to users, what groups they belong to, group structures, and resource profiles.

The Operations ID attribute allows a user to perform maintenance functions on the RACF protected system resources. (Winter) This attribute allows users to maintain certain system

resources, such as database administrators that need to update and alter RACF protected databases.

The Auditor ID attribute can be used for auditors (obviously) and security administrators. This attribute gives the user system-wide access to the RACF security controls and the reporting and logging features. (Winter)

Group-level attributes are similar to system-level attributes. However, with group level attributes, users are granted the powers of the attribute only within a particular group and any of its sub-groups. Users may have the attributes mentioned before (Special, Operations, Auditor), as well as the Connect or Join attributes. Connect allows a user to connect an existing user to a group and assign the user a group authority. The Join attribute gives users the ability to define new users and groups, as well as assign group level authorities in RACF. ("OS/390 SecureWay…")

One of the RACF security tools, DSMON (data security monitor), can produce a report that lists the users with these attributes at the system level. (Winter) It is a good security practice to determine who has these specific types of access and the reason behind having this access. Users who can not supply a sufficient reason for having these attributes, should probably have the attribute removed because each of these attributes grants significant amounts of (potentially damaging) power over the system to that user. It is also important to determine the level of logging that occurs with the use of these powerful attributes, as well as who performs the review of these logs. (Jerskey)

Group Profiles

To simplify the administration of users across the organization, RACF employs the use of group structures to give several users access to common resources. A group is a collection of users who share the need to access certain RACF-protected resources. Similar to user IDs, groups are identified by their own unique ID numbers. ("Security Server (RACF) Introduction") Along with the user IDs, the group IDs are stored in the RACF database. Since all users should belong to at least one group (and, more likely than not, belong to several), granting the proper access authorizations to each group in an organization is of utmost importance. Granting improper access to a group will give each individual user in that group the improper access. Groups may also be used to delegate security administration to resource owners. (Kimble)

Groups are usually arranged according to user function. They can be arranged in a hierarchical manner, creating a "tree" of groups across the organization with "children" groups inheriting security from their "parents." (Kimble) Groups should be arranged to provide the most minimal access to system resources necessary for its users to perform their business functions. Additional groups can be created to give users that need access to other resources the additional authorization to access these resources.

Units within an organization will often have their own groups to allow workers in these areas to use the common resources for that area. For example, to set up all of the users in an organization's accounting department, an administrator may create a general group for all accounting employees. This group is given access to the *minimum* number of resources necessary for the employees to perform their functions. This creates a "baseline" group. In this example, this group may have read access to the financial systems used in an organization, things an entry-level employee in the accounting department needs. Another group could be created to give payroll employees in the accounting group read and update access to the payroll systems. In this case, the payroll employees are connected to the accounting department baseline group, giving them read access to the financial systems, and the payroll group, giving them read and update access to the payroll functions. Since other accounting groups may not need access to the payroll applications, only those specifically needing payroll access are connected to the payroll group. Another group of employees, payroll managers for instance, may be connected to the accounting department baseline group, payroll group, and to a separate manager group. Again, the goal is to grant the least amount of privileges to the employees that allows them to perform their jobs. Having specialized groups that grant access to a specific set of resources, and then selectively connecting user profiles to these groups allows the security administrators to properly authorize access to the resources in an organization.

Managing an organization with more than a few groups can quickly become incredibly complex. Proper usage of access and group structures is necessary to keep the system's groups from becoming too complex to be effectively managed.

A common problem that arises in a structured group environment is when users from one area need access to a particular resource not normally used in their area. Using our example above, a user from accounting may need access to a particular resource used by the marketing group. The system administrator then faces the problem of how to grant access to that resource. A common practice is simply to attach the user to another existing group that has access to that particular resource. Thus the accounting user's ID may be attached to the marketing baseline group, which has the necessary access to the marketing resource.

While this solves the problem and keeps the work and the number of groups to a minimum, this also gives the user in accounting access to all of the marketing systems that the marketing baseline group has access to. This can lead to an unsecured environment where users have access to resources they do not need. Additional thought should be given to this practice. Does the user in accounting need access to all of the marketing resources connected to that baseline group, or just one particular resource? By creating a new group with access to only the one marketing resource needed, an administrator can attach the accounting user to the new group and grant the minimum access. This second strategy promotes a more secured structure, with users only having the access they need. However, this strategy creates another group that must be managed. Doing this repeatedly may create many groups that have one user and one resource,

further complicating administration. Security administrators need to weigh differences between the options and determine what is best for their organization.

Because managing the organization's groups can quickly become confusing, it is necessary to maintain standards for creating, naming, and updating groups. This should be covered in the organization's security policies and followed on a day-to-day basis by the security administrators.

Data Set Profiles and General Resource Profiles

After defining users and placing them together in groups, users need to access resources to perform their daily business functions. Data sets profiles contain security information about DASD (direct access storage devices) and tape data sets. General resource profiles contain security information about general resources, such as databases and applications, secured in RACF. Group profiles are attached to data set and general resource profiles to give all users in that group access to the data set or resource. Three profile types are used when creating data set and general resource profiles: discrete, generic, and grouped. ("Security Server (RACF) Introduction")

Discrete profiles have a one-to-one relationship with a particular resource. In other words, there is one discrete profile for one resource. Since the discrete profile allows access to one specific resource, it is commonly used with highly sensitive data. It is possible to grant access to a certain data set to only one user or group. ("Security Server (RACF) Introduction") Once a discrete profile is created to protect a data set or resource, RACF adds an indicator to the data set or resource that shows it is singly protected by a discrete profile and adds the profile to the RACF database. ("OS/390 SecureWay…")

Generic profiles are useful in one-to-many relationships. One profile can control access to one or more resources or data sets whose names have certain character patterns or strings of characters. For example, this allows an administrator to control all data sets with names that start with "SMITH." Instead of having to create individual profiles for every data set that starts with "SMITH", one profile is used that allows access to all data sets that begin with the characters "SMITH.". This is helpful when files are created or deleted with this naming structure because the existing profile works in either case. ("Security Server (RACF) Introduction") Generic profiles help keep the total number of profiles needed to a smaller number than if each resource had to be individually defined with a discrete profile. This allows the RACF database to remain smaller and easier to administer. ("OS/390 SecureWay…")

Grouped profiles are used when a simple character matching technique will not work to associate a certain set of data sets or resources with a particular profile. The grouped profile allows an administrator to associate a profile with all of the necessary resource names specifically. ("Security Server (RACF) Introduction")

Conclusion

Responsibility for securing or auditing an organization's information environment is a daunting task, even more so when the very application in use to secure it is unfamiliar. Despite RACF's widespread use in companies around the country, many security administrators and auditors know very little about it. Hopefully, after this discussion, the basic user, groups, and resources are more familiar. Understanding how user IDs are placed together into groups, which are granted access to the data and resources in an organization is vital to understanding how RACF provides security within that organization. Understanding these principles should help an administrator or auditor to become more comfortable with the RACF-protected environment.

References

IBM RACF Website. March 14, 2001. URL: http://www.s390.ibm.com/racf/

Jerskey, Pamela. "RACF Audit Program." March 14, 2001.
URL: www.auditnet.org/docs/racfaud.txt

Kimble, Richard. "RACF Security Review." March 14, 2001.
URL: www.auditnet.org/docs/RACFAuditProg.PDF

"OS/390 SecureWay Security Server RACF Security Administrator's Guide." March 19, 2001.
URL: http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/ICH1A721/CCONTENTS

"Security Server (RACF) Introduction." March 13, 2001.
URL: http://www.s390.ibm.com/ftp/books/os390/pdf/ich1a510.pdf

Winter, Mark A. "RACF Audit Program." March 13, 2001.
URL: http://www.auditnet.org/docs/racf2.txt

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event