RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 9
Issue 2
April
2015

Shorter Password Phrases

First introduced in z/OS 1.7, Password Phrases ("phrases") offer an alternative to passwords for user authentication. Phrases are 14 to 100 mixed case characters in length. IBM's sample RACF exit ICHPWX11 can be implemented to enable the use of shorter 9 to 13 character phrases.

Installing the password enhancements in APARs OA43998 and OA43999 (see RSH RACF Tips of January 2015) and activating the new KDFAES password encryption option allows use of the shorter phrases without the exit.

Also with these APARs, an ID no longer requires a password along with a phrase, and a phrase alone can be the sole means of authentication.

TSO STATUS, CANCEL, OUTPUT

The TSO STATUS command lets you monitor the status of jobs. CANCEL lets you cancel jobs. OUTPUT lets you view and purge job SYSOUT.

None of these commands provide any inherent security. Their use can only be restricted by either TSO exit IKJEFF53 or profiles in the JESJOBS and JESSPOOL classes.

z/OS is shipped with a pre-installed default IKJEFF53 module that only allows a user to act on a job whose name begins with the user's USERID. This level of protection may not be adequate. For example, if a user named Paul Rod is assigned USERID PROD, and production job names start with PROD, Paul would have access to their SYSOUT and be able to cancel them. Only JESSPOOL and JESJOBS profiles can provide appropriate protection for such jobs.

Furthermore, to allow users to manage jobs other than their own using the new JES2 Job Modify SSI 85 functions, the default IKJEFF53 module must be removed. Before doing so, implement JESJOBS and JESSPOOL profiles to properly guard all jobs and their SYSOUT.

For more on SSI 85, see article "z/OS 2.1 JES2 Modify Service" in RSH RACF Tips, April 2014.

ASG-Zeke Resource Classes

Zeke and companion product OASIS come with predefined internal resource class names for each of Zeke's 20+ resource types (e.g., Z$VAR for variables). By default, each of these internal classes is configured to use a matching RACF class. Rather than defining all these classes to RACF, an approach we have used is to create a single shared RACF class (e.g., $ZEKE), modify OASIS to reference the shared class for each resource type, and customize the resource names to prefix them with their internal class names. The one exception is Z$CATAL which is required as is.

SURROGAT Profile Owner

Some installations assign the surrogate ID as the owner of its own corresponding SURROGAT profile (e.g., ID PAYBAT is the owner of profile PAYBAT.SUBMIT). This allows any surrogate user of the ID to submit a job causing the ID to execute RACF commands which change its own SURROGAT profile. We advise using groups as owners for SURROGAT profiles instead.

AUTOPROF SMF Event Records

When FACILITY BPX.UNIQUE.USER creates an OMVS segment for a user or group, an SMF record with event AUTOPROF will be generated provided SETROPTS AUDIT is active for classes USER and GROUP, respectively.

Base64 Messages in RACF-L

On occasion, you will encounter messages in listserv digests and archives that look like random character strings (e.g., U2FtcGxlIEJhc2U2NA==). These are messages generated by an email client using Base64 encoding rather than simple text formatting. To decode such messages, use the

following website. Just copy/paste the Base64 text into the top block and click on <DECODE>.

https://www.base64decode.org/

INITOEDP SMF Event Records

If a user dubs into z/OS Unix using the default UID provided by FACILITY BPX.DEFAULT.USER, an SMF record with event INITOEDP will be generated. If a user with an assigned UID dubs using the BPX.DEFAULT.USER default GID, no such record is generated *unless* SETROPTS AUDIT is active for class PROCESS. This is also true for all other dubbing. RSH recommends setting AUDIT(PROCESS) to log all dubbing.

Auditors: Profile Creator Access

RACF was originally designed to add the USERID of a profile's creator to its access list with ALTER access. RACF Administrators who did not routinely remove their IDs from such access lists would accumulate inappropriate permissions.

RACF subsequently introduced SETROPTS option NOADDCREATOR to stop granting such access. To verify its implementation, look for the following in the output from a SETROPTS LIST.

ADDCREATOR IS NOT IN EFFECT

For more on auditing RACF, attend RSH's RACF - Audit and Compliance Roadmap course.

Orphaned OWNERs and GROUPs

Every Unix directory and file ("object") has a File Security Packet (FSP) which contains the UID of its OWNER. Ideally, this UID is assigned to a RACF USERID. If, however, the RACF USERID assigned this UID is deleted or is given a different UID, the Unix object will become unowned or orphaned. If the OWNER UID is later assigned to another RACF USERID, that user will inherit ownership of the UNIX object which might result in unintended or inappropriate access.

The same is true for the Group GID in the FSP. Deleting the RACF Group assigned the GID leaves the object with an undefined group that could later be reassigned.

Any installation which does not routinely check FSP UIDs and GIDs before deleting USERIDs and groups is likely to have orphaned objects. To locate such objects, execute the following find commands from the Unix shell with an ID that has READ and SEARCH (r-x) access to all directories and does not have UAUDIT.

find / -nouser
find / -nogroup

These commands are CPU and I/O intensive. Alternatively, generate an IRRHFSU unload and look for blanks in the HFSBD_OWN_UNAME and HFSBD_OWN _GNAME fields.

For more on protecting z/OS Unix, attend RSH's RACF - Securing z/OS Unix course.

For more on IRRHFSU, see the handout from our presentation which is available on our website.

RSH News

"Plan your work, and then work your plan." To build an effective plan, start with a thorough RSH RACF review. ***Call us today!***

Here is what Rich Russ of Trinity Health had to say about our WebEx training: "The 4-hour training format a day was key to absorption of the material. Best format I've ever had!"

Upcoming ***RSH RACF Training*:**

- RACF - Securing z/OS Unix
  September 22-25, 2015 - WebEx
- RACF - Intro and Basic Administration
  June 22-26, 2015 - WebEx
  December 7-11, 2015 - WebEx
- RACF - Audit & Compliance Roadmap
  November 10-13, 2015 - Boston, MA