RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 3
Issue 4

October
2009

Reducing Unix Superuser Use

Most installations have replaced the assignment of uid 0 (a.k.a. root) with READ access to FACILITY resource BPX.SUPERUSER for their Technical Support users. This enables them to *su* (switch user) to root whenever needed.

For many tasks, Technical Support users only need to examine directories and files. Yet, they almost always have to switch to root just to get read access and thereby unnecessarily acquire the power to inadvertently disturb objects.

To reduce the need to su to root, permit your Technical Support users READ access to UNIXPRIV SUPERUSER.FILESYS. This will enable them to read all directories and files but not modify or delete them. Only if they intend to change something would they need to su to root.

Should You Monitor or Restrict LISTDSD, RLIST, & SEARCH?

By design, RACF does not create SMF records for any use of LISTDSD, RLIST, or SEARCH. Yet, we have found these commands to be among the best hacking tools for probing RACF defenses during a penetration test. If I want to know if I can access a particular APF-authorized library, all I need do is execute:

```
LD DA('APF-library-dsname') GEN
```

If I am permitted access, LISTDSD will list information about the protecting profile including my level of access, WARNING, and AUDITING. If not, it will issue a message stating I am not authorized to list the profile while helpfully telling me what profile I am not allowed to list.

This same behavior holds true for the RLIST command. For example, I could find out if I am permitted access to FACILITY STGADMIN resources governing the use of powerful storage administration functions. Similarly, SEARCH will list all the profiles matching my selection criteria to which I am permitted access at some level. All this can be done without alerting security that the system is being probed.

Only RACF administrators and auditors typically use these commands on a regular basis. Use by anyone else should possibly be investigated.

If you wish to monitor or restrict the use of these commands, define them as profiles in the PROGRAM class. If you only plan to monitor their use, set UACC(READ) and AUDIT(ALL). Otherwise, set UACC(NONE). Specify ADDMEM('SYS1.LINKLIB'//NOPADCHK) and include any other APF-authorized libraries where copies are kept. Remember to define both the command and its abbreviation (e.g., LISTDSD and LD). If monitoring, generate and review reports of their use on a regular basis.

List All SETROPTS Options without System-AUDITOR

Do you have users who need to be able to execute SETROPTS LIST to simply view all the RACF options? Just connect them to a group with Group-AUDITOR authority. Any group will do. You could even create a special standalone group (no subgroups, users, resources, or permissions) named something like SETRLIST just for this purpose and connect users thusly:

```
CO userid GROUP(SETRLIST) AUDITOR
```

SMF Unload LRECL Change

APAR OA26653 "NEW FUNCTION - RACF SMF DATA UNLOAD UTILITY SUPPORT FOR WEBSPHERE TKLM AND EIM REMOTE AUDIT SECURITY RECORD" increases the SMF unload output LRECL from 8192 to 12888. If you specify a shorter LRECL, IRRADU00 automatically changes it to 12888. None of this is mentioned in the APAR. This could pose a problem if you have other jobs or job steps that process the SMF unload output and expect an LRECL of 8192. Be sure to update your jobs to use the new LRECL before applying this APAR. See APAR OA30046 for more details.

*Auditors: Review Access Permitted to **

When inspecting default access, it is necessary to look beyond a profile's UACC (Universal Access). UACC is the access granted to all users, even those executing without a RACF defined ID. UACC is only half the story.

Default access can also be granted to just the RACF defined users. This is accomplished by permitting access to ID(*). Access permitted to * is the same as access defined for the UACC except that it is not extended to undefined users. In most RACF environments, nearly all users have a RACF ID, so for all practical purposes access permitted to * is the same as UACC.

A few years ago at the height of the SOX frenzy, auditors were demanding all profile UACCs be set to NONE. Many security staffs complied by setting UACCs to NONE and granting access to *. While this change met the auditors' explicit requirements, it may not have met their intent.

When permitted access, * appears in the profile's standard or conditional access list along with the permitted level of access. To view a profile's access lists, add operand AUTH or ALL to your LISTDSD or RLIST command like this:

```
LD DA('dataset-profile') AUTH
RL class profile ALL
```

If you have access to a RACF database unload file or an adjunct RACF administration product, you should be able to generate a report of all permissions to *.

While we recommend the use of * instead of UACC for granting default access, the difference in terms of additional protection and control is miniscule. We suggest you closely scrutinize all such permissions.

Restrict Use of DSMON

The DSMON utility provides valuable information about the status of your controls and can identify certain vulnerabilities. To execute DSMON, you either need System-AUDITOR authority or, if the DSMON program ICHDSM00 is protected by a PROGRAM class profile, you instead need READ access to the corresponding profile. If you previously created a PROGRAM profile of * or ** with UACC(READ) to meet the control needs of z/OS Unix but failed to also define a profile specifically for ICHDSM00, you have probably opened use of DSMON to everyone. Be sure to protect it by creating a more specific PROGRAM profile with UACC(NONE).

RSH News

Has an RSH RACF Tips article helped you? If yes, kindly tell us.

Have you seen our recent **ISACA Journal** ad? Send an email to training@rshconsulting.com by December 31, 2009 telling us the issue and page where you found it to get 5% off the admission fee to a 2010 RSH RACF training seminar.

Upcoming ***RSH RACF Training***:

- RACF - Audit for Results
  November 3-5, 2009 - Boston, MA

See our website for details and registration form.

We will be giving presentations at several upcoming RACF User Group meetings. Visit our website for meeting details and handouts.