RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 86):

This Issue's Themes:

- Better InfoSec Through Better Reports
- More Secure Passwords
- Sensible Delegation of Authority

Free Webinar "*What's Missing in Mainframe InfoSec (What We Don't Know We Don't Know)*" April 14 and again on April 20 at 2PM EST

NewEra Software hosts Stu Henderson's on why we still have so many break-ins after all the effort put into InfoSec.. For info, or to register for this free session:

http://www.newera-info.com/Stu_Henderson.html

(You can also see there handouts from earlier webinars, including "***Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In***", "***JUST FOR CIOs - Managing Mainframe InfoSec More Effectively***" and "***How to Secure Mainframe TCP/IP***")

Mid-Atlantic Security User Group (MASUG) Meets May 5, 2015

MASUG serves IBM mainframe customers. The next meeting is **May 5th, 2015 from 8:30 to 3:30** at: CA Technologies Inc. Building Suite 400, 200 Princeton S. Corp Center Ewing , NJ 08628

For info or to register, please visit https://communities.ca.com/events/1749 or email to: Paul.Rauchet@ca.com

NEW YORK RUG Meeting Date

Thursday, April 16, 2015 from 10AM to around 4PM.

Our meeting sites are at IBM in Tampa and NYC. We WILL teleconference with Tampa.

THIS IS A LOT OF TRAINING AVAILABLE IN ONE DAY. **You will not be allowed to attend without pre-registering (it's free), as described inside.** See inside for details.

(The meeting after that will be **a Fall date to be determined in 2015**)

Please Note the New Website for the NYRUG and TBRUG: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG at www.nyrug.stuhenderson.com

---

Today's Quotation

"*Gentle, constant, reliable presence is often the most beautiful gift our dear ones can give us.*"

— David Servan-Schreiber

Vanguard Conference

This great conference will be held twice in 2015. The spring event - Vanguard Security & Compliance East 2015 takes place April 27-30 at the Tampa Hilton Downtown in Tampa, FL. For more details, visit www.go2vsc.com. For more information, people can contact glory.wade@go2vanguard.com.

To subscribe to this newsletter, or for back issues:

http://www.stuhenderson.com/Newsletters-Archive.html

Making Passwords More Secure

IBM has been making major improvements in password security. Here we discuss password security assuming that someone has obtained a copy of your RACF database. (The questions to address if no one has read access to any copy of your RACF database is a separate subject, to be addressed in a later issue.)

The free, well-known password cracker program John the Ripper has now been enhanced to crack RACF passwords, so it then becomes just a matter of time before all of your userids and passwords are known. How long? That depends on the encryption used and the length of the passwords. You can get an idea from Peter Goldis password cracker emulator, as described in Issue 80 of this newsletter (http://www.stuhenderson.com/RUGNEW80.pdf) You'll see there how under constant conditions, the estimated time to crack a password goes from seconds to hours to days as the length of the password increases to 8. (Under other conditions, such as faster CPUs, cracking speeds may be faster.)

To give hackers a harder time, IBM is improving the encryption algorithms and making it possible to require password phrases without having passwords. Improving the encryption algorithms is a good thing, but best left for mathematicians to explain. The password phrases is easier to understand.

IBM added password phrases (with lengths up to 100 characters) to RACF to make it harder for hackers to guess. (This may also have been in response to auditors with Windows-based checklists requiring password lengths of 14. This is a good thing to do in Windows because of a bizarre weakness in Windows password handling, which we will not discuss here.)

When IBM added password phrases to RACF, IBM required any userid with a password phrase to have a password as well. You could then require users to use password phrases by not telling them their passwords. But hackers with a copy of your RACF database would ignore the phrases, since the shorter passwords are much easier to crack. So IBM is now letting us have userids with password phrases without passwords. Implementing this will give us greater protection should a hacker get a copy of our RACF database.

Please note however, that it's still just a matter of time. Say it takes a password cracker program on average seven days to crack a password or password phrase from your RACF database. Then how long do you think your password interval should be?

So proper evaluation of password risk should include all together: what encryption is used, minimum password / phrase length, password interval in days, and how well we prevent access to any copy of the RACF database. With the current developments, this might be worth re-visiting. And thanks, IBM.

Want to Have More Special Characters in Your Passwords?

You can with **SETR PASSWORD(SPECIALCHARS)** (after applying APARs OA43998 and OA43999). These will also give you stronger passwords and better overall security. Note that some special characters may cause problems with certain sign-on screens or ISPF panel fields.

This Issue's Featured Resource Class: WRITER

As with most resource classes, the key to understanding WRITER is to understand what software calls RACF, and what it does with RACF's response. The RACF calls in the WRITER resource class are made by JES (either JES2 or JES3). JES is the system software that manages JCL, batch jobs, started tasks, and printouts. When a program wants to send data to a sysout printer, JES intercepts the write request and saves the data to be printed to a disk file called the SPOOL. When your JOB finishes, JES writes the data from the SPOOL file to the appropriate printer.

(JES can also send the printout over the network via NJE or RJE to be printed elsewhere.)

Before sending the printfile to a local printer or over the network, JES calls RACF in the WRITER class, asking if this user should be allowed to send printouts to that destination. (The SDSF software also calls RACF for the WRITER class, for similar purpose.)

To decide whether and how to use the WRITER class, your organization needs to assess the associated risk. If you have a printer dedicated to printing checks all day long on pre-signed check stock, the risk will be greater. If you have sensitive data that could be accidently or deliberately sent without authorization to a remote printer, then the risk is greater. The team making this risk assessment should likely include at least the RACF administrator, the JES system programmer, the Compliance or Legal department, and the owners of the data. Your JES sysprog can tell you the names of the local and remote printers, and where each is located.

Note that the WRITER class can be used to control batch jobs as well as printouts sent over NJE and RJE. Use the WRITER class for outbound batch jobs and printouts. Use the NODES class for inbound.

If you want to collect information on use of WRITER in your shop, you could create backstopping rules (named for example **) which allow but log every access. Coordinate this with your JES sysprog to minimize the amount of SMF records you generate. (For example make one rule for all local printers without logging and a second rule for all remote printers with logging. Or turn on the logging just for ten minutes to see the volume of SMF records, and then fine tune from there.)

Free Sources of Useful Guidance for InfoSec

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository
- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53
- Handouts from previous meetings of the NYRUG: http://www.nyrug.stuhenderson.com/handouts.HTM

New Keyword on RACDCERT Command Helps Manage Digital Certificates

If you want to list a digital certificate and learn what keychains it is part of, the LISTCHAIN keyword will help you out. Issue:

RACDCERT xx LISTCHAIN LABEL('labelname')

where **xx** is one of **ID(userid)** or **CERTAUTH** or **SITE**. The result tells you all the chains the certificate is a member of, all the certificates in each chain, whether each certificate is TRUSTed or not, and whether each chain is complete. A nice tool to make PKI easier for us all.

Protecting Against Two Ways a Hacker Might Attack Your System

Sometimes an indirect attack is more effective. Suppose you have a started task marked TRUSTED to RACF. (See the Started Procedures Table in the DSMON report.) RACF allows it to do anything it wants (more powerful, some say, than OPERATIONS). You make the userid of the started task protected (no password) so no one can log on using it. You think you have protected this powerful started task, not realizing that many users have UPDATE access to the proclib dataset where the JCL for the started task is stored. Anyone who can update this proclib can change the JCL for the started task to execute any program he or she wants.

This means that you want carefully to control who can update proclibs, perhaps with auditing of any updates to them. And to do this, you need to know the names of all the proclibs. (They may be several beyond SYS1.PROCLIB. Ask your JES sysprog for a complete list, and to keep you informed of any changes.)

A second indirect attack would consist of updates to the RACF parameter library. Any operator command issued from here is not protected by rules in the OPERCMDS resource class. So add this dataset to the list of system datasets that need to have updates tightly controlled and reviewed (along with the proclibs, the parmlibs, the APF libs, and others).

If you consider the head of the Payroll department to be the "owner" of the Payroll application datasets, then you might consider the system programming manager the "owner" of all the system datasets. If an auditor were to look at the dataset rules protecting system datasets, would there be a set of written approvals he or she could use as a standard to compare to? If you (or the system programming manager) don't provide a standard, what standard do you think the auditor is likely to use?

What Does Group-SPECIAL Mean?

Group-SPECIAL is a way of delegating authority in RACF. It helps to think of two types of RACF authority: Type 1 is the ability to ADD a new record to the RACF database. Type 2 authority is the ability to ALTER or DELETE an existing record in the RACF database.

There are three basic ways to give a user Type 2 authority over an existing rule in RACF:

- Give her userid SPECIAL (that is, User SPECIAL, aka System SPECIAL)
- Make her userid be the owner of the existing rule
- Give her userid Group-SPECIAL over the existing rule

In other words, having Group-SPECIAL over something is very much like having your userid be the owner of it. The difference is that several users can have Group-SPECIAL over a rule at the same time. In contrast, if a rule is owned by a userid, it can only be a single userid at a time.

Yet another way to think of this is to consider Group-SPECIAL a way to let several userids “be the owner” of a rule at the same time.

To understand how to give a userid Group-SPECIAL over an existing rule, it helps to understand the RACF Group Tree. You can see what it looks like in the DSMON report titled RACF Group Tree Report. A user connected to a group with Group-SPECIAL has type 2 authority over that group, all the groups it owns, all the groups they own, and so on down the tree, so long as a group owns a group owns a group. This user also has type 2 authority over every userid, dataset and resource rule owned by any of these groups, as well as dataset rules with these groups and userids as the high level qualifier.

Why Controlling Batch Job Submission is Important

Unless you know that all of the UACCs on all of your dataset and resource rules are set to NONE (or at least to something safe), you run this risk: someone runs a batch job that takes advantage of a loose UACC to copy or change data without being authorized. To reduce this risk, you want to prevent anyone from running a batch job unless that person has a valid RACF userid. Here are some steps you can take:

1. Make sure that both **BATCHALLRACF** and **XBMALLRACF** are active (see SETR LIST to be sure)

2. Make sure that every **UACC** is **NONE** (using permissions with **ID(*)** to loosen this, since ID(*) applies only to programs running under a valid RACF userid). To verify that every dataset UACC is none, you might use the RACF ICETOOL with an EXEC card like this:

   //STEP1 EXEC RACFICE,REPORT=UADS

3. Control all the paths through which batch jobs can enter your system. Include NJE, RJE, FTP.

4. Make all automatically assigned userids protected (no password, no OIDCARD), so they can’t be logged onto by guessing the password. This includes all userids for started tasks, consoles, and production batch jobs.

5. Make all userids which do not belong to people or to critical started tasks be RESTRICTED, which prevents them from accessing datasets or resources by means of UACC, ID(*) permission, or the GLOBAL table (listed in the DSMON report). Consider making RESTRICTED all those userids used for unidentified users, for example userids automatically assigned by TCP/IP daemons to permit the general public to read your organization’s ads over the Internet. (Ask your TCP/IP administrator or WAS administrator to keep you briefed on these.)

Wait, What's This About RACFICE or ICETOOL?

RACFICE (also called ICETOOL for RACF) is an IBM-supplied tool that produces very useful, well-formatted, and tailorable reports from the RACF database and/or your SMF data. If you have RACF, it costs you nothing. Here's how it works for reports based on your RACF database: Each night, right after taking backups of the RACF database, you have a batch job that runs the RACF Database Unload Utility (named IRRDBU00). This reads a copy of the RACF database and produces a flat file that has all the information from the database (except no passwords) formatted in a very easy to read layout.

Then when you need a report, you run a batch job with

//STEP1 EXEC RACFICE,REPORT=xxxx

where xxxx tells the program which records to select from the flat file and how to format the resulting report. For example, **REPORT=UADS** tells RACFICE to select only the names of dataset rules with a UACC other than NONE. It also tells RACFICE what fields from these dataset rules to print in the report, and how to format these fields.

You can learn more about RACFICE in the IBM manual "***RACF Auditor's Guide"***. This will also tell you how to use RACFICE to report against SMF data for RACF too.

Do You Regularly See This Useful Information Reported by RACFICE?

Below are some often-ignored reports from the RACF database that will help you be a better RACF administrator. RACFICE is of course just one of the tools (including the SEARCH command) that can provide you this information. However you get it, you will want to review the following on a regular basis:

- Dataset and resource rules which are discrete, but which have * or % in their names
- Dataset and resource rules with either UACC or ID(*) permission greater than NONE
- Dataset and resource rules with WARNING
- Dataset rules with ERASE(YES)
- Userids connected to a group with AUTH greater than USE
- Number of rules by type: user, group, dataset, and resource broken out by resource class (identifies unauthorized additions and changes, suggests performance tuning)
- Number of dataset rules broken out by High Level Qualifier
- Userids with NOINTERVAL (so they don't have to change their passwords)
- Userids with USS UID zero
- Userids with duplicate USS UIDs other than zero

But Wait, None of Those RACFICE Reports Gives Me What I Need

That's OK. RACFICE makes it easy to define your own selection and format, or to modify the ones IBM supplies. See the "***RACF Auditors Guide***".

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet April 16, 2015 from about 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa. This is a joint meeting by teleconference with the NY and Tampa FL RUGs.

Attendees **must present a government issued photo ID** to enter the IBM building. Admission is free, but even if you have registered for previous meetings, you must pre-register by emailing NO LATER THAN NOON the day before.
For Complete Directions, geto copies of handouts and to register, please visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.

HG RACF Training Schedule:

The Henderson Group offers its RACF and information security/audit seminars around the country and on-site too. See the details below or call (301) 229-7187 for more information. For detailed class descriptions or to see what students say about these classes, please go to www.stuhenderson.com/XSECTTXT.HTM. (See info on Mainframe Audit classes below.) You can save money by holding a class session in-house, or by hosting a public session. Contact Stu for more info.

1) HG04 **Effective RACF Administration** (**$2195**)
December 1-4, 2015 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
Dec. 7-10, 2015 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 9, 2015 in Bethesda, MD

HG Mainframe Audit Training Schedule:

The Henderson Group now offers its series of "How to Audit.." seminars for IS auditors. These describe clearly how the associated software works, where the control points are, how to collect and interpret data, and how to conduct the audit. The workbooks include complete audit programs. More information is available at our website: www.stuhenderson.com/XAUDTTXT.HTM. (If you have a class topic you would like to have added to this series, please let us know.) (See info on "RACF Training" classes above.) You can save money by holding a class session in-house, or by hosting a public session. Contact Stu for more info

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, DB2, and MQ Series Security** (**$2300**)
September 21-24, 2015 in Chicago, IL

B) HG65 **How to Audit z/OS with USS, TCP/IP, FTP, and the Internet**
(This class is a logical follow on to HG64.) ($1590)
Nov. 10-12, 2015 in Bethesda, MD

C) HG76 **How to Audit UNIX and Windows Security ($2200)**
June 22-25, 2015 in Bethesda, MD

Permanently Interesting Products Column

This column has been permanently moved from this newsletter to Stu's website. You can find it at: www.stuhenderson.com/XINFOTXT.HTM.

RACF User Services (Newsletter Subscriptions / Key Phone Numbers / Addresses)

Technical support hotline, Meetings, Seminar Catalogs:
Stu Henderson - (301) 229-7187
5702 Newington Rd, Bethesda, MD 20816

For Back Issues of this Newsletter, Subscriptions and Links to Several Useful Web Sites

check the Henderson Group website at:
http://www.stuhenderson.com/Newsletters-Archive.html

RACF List Server on the Internet

To join, send E-mail to the administrator for the server. (Don't send it to the server itself or your request will be routed to every subscriber.) For example, if your name is John Smith and you want to subscribe, then send this E-mail:

subscribe racf-l john smith

to the address: **listserv@listserv.uga.edu**

The reply will include directions on how to get info such as a list of all subscribers, an index to previous comments, and a command summary. You will want to set up a filter for incoming emails to direct mail from the list server to a dedicated folder or directory.

Free Email Newsletter for Mainframe Auditors

To see back issues or to subscribe to the Mainframe Audit News (MA News), check Stu's website at
http://www.stuhenderson.com/Newsletters-Archive.html

To Get a Free Subscription to the RACF User News Or to see back issues: check Stu's website at
http://www.stuhenderson.com/Newsletters-Archive.html

The RACF User News is published two times a year to share information about RACF. All information in it is offered on an "as is" basis, and should be used at your own risk, and with your own testing.

Another Source of Free, Practical Info:
Here are links to lots of useful info, including: a mainframe glossary, vendor integrity statements, z/OS configuration information, audit guides, and more.

www.stuhenderson.com/XINFOTXT.HTM

Other Internet places:

- RACF Password Cracker Program. Email Peter Goldis at **pete@goldisconsulting.com** or look at **www.goldisconsulting.com**
- Nigel Pentland's security page is www.nigelpentland.co.uk
- IBM RACF home page: www.ibm.com/servers/eserver/zseries/racf/
- RACF goodies site: www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html
- RACF Presentations Page with lots of presentations from SHARE and GSE. Check out http://www.ibm.com/systems/z/os/zos/features/racf/presentations.html
- IBM Redbooks site: www.ibm.com/redbooks
- IBM z/OS Manuals: www.ibm.com/servers/eserver/zseries/zos/bkserv/
- Net-Q Enterprise Extender Security case studies and examples at www.net-q.com.
- (Other vendors contact info listed in the "Permanently Interesting Products" column which is now moved to Stu's website at:**www.stuhenderson.com/XINFOTXT.HTM**
- the Henderson Group: **www.stuhenderson.com**

21 Things RACF Auditors Should Know:
This PDF file lists 21 things for auditors, including a reference on why you don't need to protect the program AMASPZAP with RACF. The article is available at:

www.stuhenderson.com/XARTSTXT.HTM

More Info on Tape Security and RACF
is available at
www.stuhenderson.com/TAPESEC1.PDF

"Why RACF, ACF2, and TopSecret aren't sufficient for effective tape file security" describes how to get full security for tape datasets by using both security s oftware and tape management software