RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 70):

NEW YORK RUG Meeting Dates

Thursday, May 3, 2007 from 10AM to around 4PM. PLEASE NOTE THIS IS A SPECIAL MEETING WITH DIFFERENT TIMES AND REGISTRATION REQUIRED. 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. Mark your calendars now. See inside for details, including the tentative agenda. The meeting after that will likely be in October, 2007. Please note the NYRUG will meet twice a year from now on.

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

NY Metro NaSPA Chapter (system programmers professional association) meets Tuesday, 24 April 2007 in room 1219 at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM. You are warmly invited. Details inside.

More Info on Tape Security and RACF is available in the following article from the zJournal:

http://www.zjournal.com/index.cfm?section=article&aid=762

Todays Proverb **"When what you're doing doesn't work for you, try something else.."**

Vanguard Conference in St. Louis in 2007
It's scheduled for June 10-14, 2007 in St. Louis, MO. For details, go to www.go2vanguard.com .

To Get a Free Subscription to the RACF User News Phone Stu at (301) 229-7187 with your request, leaving your name, postal address (sorry, only US postal addresses; others will need to read issues online), and phone. For back issues and articles on topics like the **SERVAUTH** resource class, check his website: **www.stuhenderson.com**

The Real Skinny on Passwords:

Some people spend a lot of time and energy arguing what the password syntax and other rules should be: “Let’s make the minimum length be 8, and NO VOWELS”, “No, no, that’s too easy to guess, make it be all numeric, but with a minimum length of 5", “Make the limit on invalid passwords be 5 so that if my finger slips, I can get another chance.”, and “Why don’t we have the RACF administrator review the violations report every day and then he can go talk to the people who keep forgetting their passwords. “

It’s easy with all these possible tools in hand to forget what really matters: “how do we make it so **passwords are easy to remember but difficult to guess”**. No matter what you make the rules, or whether you install an exit to prevent use of certain words as passwords, people will continue to do what what humans do.

If a typical user is working on a project, and the computer insists that his password has expired and he has to enter a new one, he will consider this just an interruption in his getting his job done. He will continue focusing ALL of his attention on getting HIS job done, and no attention at all to what he types in as a password.

That is, unless you teach him a process that is easy to do, almost automatic after he does it a few times, and easy to remember. One possible approach is to train users each to have his own secret formula, such as,

- “Whatever word I use as my password, I always put the number five after the third letter”
- “I put the number five as the first position of the password, the first time, the second position the second time, and so on.”
- “I change the number I insert so the first time it’s the number of the current month, or the number of the current month minus 3, or the first digit of my phone number (or tax id number or license plate number or other easily remember number) the first time, the second digit the next time and so on.”

The brief process of working out the formula will help each user to remember what he set his password to be. As long as no one else knows his secret formula, then it will be harder for hackers to guess his password.

You could teach users other techniques (such as taking the first letter of each word of some well known phrase), but the important thing is that they follow some system of their own that makes it easier for them to remember their passwords, but harder for hackers to guess.

If you are wondering whether your installation needs to consider an approach like this, try plotting over time the number of password resets each week, either as an absolute number or as a percent of all users. Consider the cost of resetting these passwords. See if the trend is increasing or decreasing. Based on what you know, estimate whether you think most passwords would be easy to guess. This is probably one of the greatest areas of security weakness in RACF shops, and you can make it better.

And of course, don’t forget to consider use of mixed case passwords and passphrases, aka password phrases. But only after you’ve trained users in how to deal with these, and made sure that all the software that asks users to enter a password can handle the new rules.

More on IMS Security:

If you suddenly need to implement RACF security for IMS, here's some basic stuff to know. The latest releases of IMS call RACF for every signon and for every transaction. You can use the APPL resource class to control who can sign onto the test region and who can sign onto the production region (just like CICS!).

IMS uses two resource classes in RACF to protect transactions, **TIMS** and **GIMS**. TIMS is just like TCICSTRN for CICS, and GIMS is just like GCICSTRN.

As with CICS, you can change the names of the resource classes IMS uses. The first letter still has to be **T** or **G**, but the IMS part of the name can be changed in a given region.

A third resource class is named AIMS, and it is used for application group names. Ask your IMS sysprog to describe how to use these.

Several other resource classes have names consisting of one letter followed by **IMS**. Your IMS programs have to request that IMS call RACF for these. They often represent parts of the database structure.

A good starting point is to make sure that all the IMS users have RACF userids (and that they are trained in how to make passwords easy to remember but difficult to guess). Ask the IMS sysprog for the names of the APPLIDs of the IMS regions, and whether they should be controlled with the APPL resource class.

Ask your sysprog to give you a list of all the IMS transactions, either alphabetically listed or grouped according to who is allowed to use them. Start evaluating whether you want to define the RACF rules with wildcards (like asterisk or percent sign) or in grouping rules (using the GIMS resource class). Remember that each transaction should be defined in either one TIMS rule or in one GIMS rule, never in both places, and never in more than one rule.

Define groups of users who can execute given transactions and permit the groups to the TIMS and GIMS rules. This way, when there is a change to the rules, you can connect/remove a userid to/from the group and you don't have to refresh the RACLIST. (This too is just like CICS.)

Make sure that for application related transactions (as opposed to system transactions) you identify the **owner**, that is the person who approves which users can use which transactions. Get the permission approval forms and annual certification set up, the same way you would with for example, production payroll dataset rules.

How You Can Get Rid of Most Userids with OPERATIONS:

It's common that a system programmer or a DASD space administrator believes that she needs OPERATIONS. The first time RACF stops her from doing her job, she'll want OPERATIONS, so it can never happen again. You may want to reduce the number of userids with OPERATIONS, but not be able to argue with system programmers who say "I need it to do my job". Here are three things you can do to minimize the need for OPERATIONS. Once you have them in place, let someone else make the decision on who gets OPERATIONS.

1) Use the DASDVOL resource class to permit authorized users to erase disk datasets without letting them read or write the datasets. The names of the rules are the volser numbers of the disk packs, if you want to permit the group DASDMGT to erase a dataset on any disk pack, issue:

   RDEF DASDVOL ** UACC(NONE)
   PE ** CLASS(DASDVOL) ID(DASDMGT) ACC(ALTER)

   DASDVOL is not used with SMS managed volumes, but you can still use it for any non-SMS managed disks. It can also be used to permit userids to do full pack dumps and restores with DFDSS or FDR without letting the users read or write the data. This class is also used by the program ICKDSF.

2) Create rules in the FACILITY resource class to permit DASD space managers to do their functions without needing operations. Most of these rules have names beginning **STGADMIN.** You can learn more by looking in the IBM manual

   DFSMS Storage Administration Reference, SC26-7402 available at

   http://publibz.boulder.ibm.com/epubs/pdf/dgt2s250.pdf

3) Ask DASD space managers to set up started tasks with distinct userids to perform basic functions like dumping a disk pack to tape. Then give these userids the authority they need to do the job, so the userids which represent actual people won't need the privileges.

Here are several things you can do to collect information on how often people really need it to do their jobs (You don't have to take OPERATIONS away from them, this is just collecting information and laying groundwork for any decisions someone might make in the future.)

A) Issue **SETR OPERAUDIT** to log every time someone does something he's only able to do because he has the OPERATIONS attribute. Get daily reporting on this off the SMF data and keep a history.

B) Consider setting up a Firecall userid, an id with OPERATIONS and SPECIAL and UAUDIT whose password is kept in a safe in the computer room. Anytime there is a system problem, right after phoning the sysprog for help, the shift supervisor opens the safe, takes out the password and gives it to the sysprog.

C) Work with DASD space management staff to define rules to let them do their functions without their needing OPERATIONS, as described in 2) above.

New York System Programmers Meet April 24 at IBM

The next meeting of the NY Metro NaSPA Chapter will be on Tuesday, 24 April 2007 in room 1219 at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM. Sessions for the day include:

- Jeff Bland, IBM z/OS Development, "IBM Migration Checker and EPSPT"

- Scott Marcotte, IBM zFS Development, "An Introduction to zFS"
- David Raften, IBM, "Avoiding Perplexation About Sysplex: It's as Easy as A. B, CF!"
- Elpida Tzortzatos, IBM z/OS Storage Management Design (ASM, RSM, VSM) " "Storage: This time it's for Real - The Real Storage Manager's Evolution for Scalability and Performance"

Pre-registration is requested and recommended as it simplifies getting into the building and helps us get the room set up correctly. Please RSVP to markan@us.ibm.com as soon as is possible if you are thinking of attending.

The meeting is open to non-NaSPA members and is free! Please pass this invitation on to your colleagues!

Why It Matters Where Decisions Get Made:

Some Scenarios:

1) The head of the payroll department discovers that there are 35 people he doesn't know who can read the payroll data.

2) The marketing vice president says to the RACF administrator: I've got 12 new employees starting next week who will be working with Mary. Give them userids that can do whatever Mary can do.

3) The form for new userid requests has room for the signature of the supevisor of the user, along with a space to specify what data and resources the userid should have access to.

4) So the auditors come by and write up findings that "too many people can read the payroll data" and "several system programmers have the SPECIAL attribute on their userids when it does not appear to be appropriate to their duties" and "35 userids have the OPERATIONS attribute. This is too many." and a recommendation that the RACF administrator review the violations report every day.

5) The resource classes VTAMAPPL and SERVAUTH are not active, but in many people's opinion are necessary for comprehensive security..

Who gets blamed here? By default, these are all problems for the RACF administrator, since they deal with mainframe information security and you are in charge of that. In each case though, the decision making that led up to the situation was made by someone other than the RACF administrator, who has lots of responsibility, but little authority.

A simple structure that eases many of these problems is to assign responsibility for APPROVING access or privileges to someone other than the RACF administrator. The RACF administrator can't make this happen; it has to come from above. But when this happens (perhaps your auditors can help influence management to make this happen), the RACF administrator's job changes: You are carrying out decisions made by other people, by the people who best understand the associated risk.

You'll have better security too.

So consider having an owner for each of these, the same way the head of the Payroll department is the owner of the Payroll data: the SPECIAL attribute, the OPERATIONS attribute, and each resource class. Then report annually to each owner who can access his stuff, so he can make changes, sign it, and return it to you.

User Group Survey

In order to help RACF User Groups, especially the NYRUG, to serve members better, we'd like to get your opinion on what you want from your user group. Please feel free to fill this out and fax or mail it to us. We will gladly share summaries with the leaders of other RUGs. All questions are optional. Thanks for your help.

1) How important is each of these to you, with **3 being MOST IMPORTANT** and **1 being LITTLE OR NONE**?

a)	Getting free technical training	1a) _____
b)	Networking with peers	b) _____
c)	Hearing what others are doing	c) _____
d)	Chance to get answers to questions	d) _____
e)	Like to get out of the office	e) _____
f)	Other (please describe) _____	f) _____

2) What topics would you like to have addressed at a RUG meeting (CICS? DB2? Digital certificates? SDSF? How to deal with the politics? Cleaning up the RACF database ? Other user experiences? Clever techniques for RACF administration? Updates on latest RACF features?)?

3) Which RUG do you belong to?

4) Please name one or two things you would like from your RUG that you are not getting now, or which you would like more of?

5) What speakers would you like to hear at a RUG meeting?

6) (Optional) If you would like to be contacted about any of this, feel free to give us your name and phone or email.

7) (Optional) How many user profiles are in your RACF database? How many dataset?

Please make sure your answers are easy to read.

Please fax this page to (301) 229-3958 (no cover sheet needed) or mail to:

Stu Henderson, 5702 Newington Road, Bethesda, MD 20816

Thanks for your help.

HG How To Audit Training Schedule:

The Henderson Group now offers its series of "How to Audit.." seminars for IT 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. (If you have a class topic you would like to have added to this series, please let us know. (See info on "RACF and Security" classes below.)

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$1550**)
May 7-9, 2007 in Raleigh, NC
Nov. 14-16, 2007 in Clearwater, FL

B) HG65 **How to Audit z/OS with USS, TCP/IP, FTP, and the Internet**
(This class is a logical follow on to HG64.) ($1560)
May 16-18, 2007 in Bethesda, MD

HG RACF and Security Training Schedule:

The Henderson Group offers its RACF and computer security/audit seminars around the country and on-site too. See the details below or call (301) 229-7187 for a free seminar catalog. For more info or to see what students say about these classes, please go to **www.stuhenderson.com**. (See info on "How to Audit ..." classes above.)

1) HG04 **Effective RACF Administration** (**$1995**)
Sept. 17-20, 2007 in Vienna, VA
Feb. 26-29, 2008 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($1990)**
March 3-6, 2008 in Clearwater, FL

3) HG06 **UNIX (USS) for RACF Administrators** (**$490**)
May 15, 2007 in Bethesda, MD

NYRUG (New York RACF Users Group):

Our next meeting is at IBM, 590 Madison Avenue. Attendees **must present a government issued photo ID** to enter the building. Admission is free to hear these great speakers, but you must pre-register by emailing NO LATER THAN NOON May 1, 2007 to Mark Nelson (markan@us.ibm.com) with "NYRUG MEET" in the subject line and your name and company in the body. Pre-registration is highly recommended.

Our exact agenda is not certain at press time, so you might want to check this link for exact details as they become final: **www.stuhenderson.com/XNEWSTXT.HTM#nyrugref .**

Starting roughly at 10AM (tentative agenda) ending around 4PM:

1. XML, Walt Farrell, IBM
2. MQ Series and RACF, Stu Henderson
3. IBM Encryption Services for z/OS, Saheem Granados, IBM
4. Surviviing a RACF Audit, Jeff Loewenstein
5. JES2 and RACF, Tom Wasik, IBM

(Please note that times are approximate and that speakers and topics are subject to revision.)

Time: **May 3, 2007 from 10AM to around 4PM**
Place: **IBM, 590 Madison Avenue**. Attendees must present a photo ID to enter the building and must pre-register in advance.

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.**

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

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

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

check the Henderson Group website at:
www.stuhenderson.com

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 learn more about the Mainframe Audit News (MA News), check Stu's website:
www.stuhenderson.com .

The RACF User News is published two times a year (March and September) 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.

Other Internet places:

- RACF Password Cracker Program. Email Peter Goldis at **pete@goldisconsulting.com** or look at **www.goldisconsulting.com**
- Georgia RUG at www.garug.net ..
- Steve Neelands's RACF page is **www.geocities.com/steveneeland/**
- Thierry Falissard's RACF page is **www.os390-mvs.freesurf.fr/**
- Nigel Pentland's security page is www.nigelpentland.co.uk
- IBM RACF home page: www.ibm.com/servers/eserver/zseries/racf/
- IBM RACF goodies site: www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html
- IBM Redbooks site: www.ibm.com/redbooks
- IBM z/OS Manuals: www.ibm.com/servers/eserver/zseries/zos/bkserv/
- (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**