RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 74):

A Tip From the RACF List Server:

Some installations follow the practice of revoking a userid by date instead of just revoking. This leaves an indication in the user record of when the userid was revoked.

How to Tell When Your Release of RACF Goes Off Service:
Google these keywords:

z/OS release support date

and follow the link to the IBM-supplied page that tells you when you have to get onto the next release to stay with IBM support.

Discount on William Data Systems for Monitoring, Security, and Control of TCP/IP and APPN Networks:
The offer is a 50% discount on any of their software valid for 6 months from 21st April 2009. This offer is exclusively available to RACF User Group members in the USA. To obtain this discount you must go to

www.willdata.com/zen_productdownload_racfug.aspx

for the terms and conditions and complete the download form. You must complete the "How did you hear about William Data Systems" drop down with "RACF User Group"

NEW YORK RUG Meeting Dates

Tuesday, April 21, 2009 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. Please note that this meeting will be the first public announcement of a new mainframe security opportunity to leave a door open (and how to close it) recently discovered by researchers at the General Accountability Office (GAO) mainframe security lab in Washington, DC. (See David Hayes' presentation.) The meeting after that will likely be in October of 2009.

NY Metro NaSPA Chapter (system programmers professional association) meets on Wednesday March 25, 2009, at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM. You are warmly invited. Please RSVP to Mark Nelson at markan@us.ibm.com

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

Vanguard Conference in Los Angeles in 2008

It's scheduled for May 31-June 4, 2009 in Jacksonville. FL. For details, go to www.go2vanguard.com .

Today's Quotation

"*If it seems you are taking one step forward and two steps back, put it to music and dance*."

Debugging RACF Performance Problems:

A recent posting on the RACF List Server (see last page of this newsletter to subscribe) led to an interesting debugging problem. It ended up illustrating some philosophy of debugging, as well as some useful information on CICS and RACF.

Here's the background: A subscriber to the list asked for technical help. Management had said that there was a serious performance problem with RACF that needed to be fixed right away. It had to do with I/O to the RACF database.

Several people on the list offered lots of good suggestions, including the idea of reporting from the SMF data the number of RACF functions occurring each hour. (These functions or "events" include **RACINIT** (checks userid and password), **RACHECK** (says whether a user can access a given resource or dataset), each of the RACF commands, and other items.)

The idea beyond the suggestion was to isolate whether there was a problem in RACF itself (which seldom happens) OR some program calling RACF so many times that it hurt performance. Also, if the problem was the number of calls to RACF, then the SMF data would tell us what type of call, and what program was making the call.

The results showed during the times of the performance problem, there were more than 11,000 **RACINIT**s per minute. This is a very high number and could explain the cause of the problem. (Note: We also learned from the List that TSO signons and batch jobs do not cut type 80 SMF records for RACINITs; although they do cut type 30 records.) CICS and other software do cut type 80 SMF records for **RACINIT**s, with an event code indicating that the event was a **RACINIT**. This record also includes a qualifier code telling you whether the **RACINIT** was successful or not, and if not, the reason for the failure.)

These 11,000 **RACINIT**s in a minute could not have been caused by human hands (unless you had the proverbial 11,000 monkeys all trying to log on at the same time). So the RACINITs had to be issued automatically by some program. The SMF records indicated that the program was CICS.

At this point in the debugging process, several subscribers suggested that the cause could be an improper value for either the **USRDELAY** or the **ATTACHSEC** fields in CICS. (Details on how these work in the next section.) It was found that the value of **USRDELAY** had been set to zero. Setting it to a value of 5 minutes alleviated the problem.

(Phil Emrich pointed out that the default value for this field is 30 minutes which would be an even better value than 5 minutes. We hope that Phil's employer doesn't find out how much time he spends on the Internet giving away free advice. He could get in serious trouble.) The next section describes what was going on in CICS to cause the problem. It's a little technical, but every RACF administrator should know something about this stuff.

Some CICS Technical Stuff You Should Know About

(Edited from advice provided by a lister)

Note that RACINIT is the RACF function that checks out your userid and password.

" I agree with the comments from others that this many RACINITs is probably not generated by human fingers, and that you might want to look first at **MRO** or **ISC**. These are ways of configuring CICS so that all users log onto one CICS region, the **TOR** or Terminal Owning Region, (which causes one RACINIT), and then when they type in a transaction name, the **TOR** sends the transaction to execute in another CICS region called the **AOR** (Application Owning Region). If the **AOR** needs to read a file, it may send the request to yet another region, an **FOR** (you guessed it, File Owning Region).

When the **AOR** receives the request, it usually does two RACINITs, one for the happy user sitting at the terminal, and a second one for the userid of the **TOR**. This is so that the AOR can ask for each of these userids "Can this user do this transaction?"

Two CICS settings affect this: **ATTACHSEC** and **USRDELAY**

ATTACHSEC determines the rigor (and the overhead) of the security handshake between the TOR and the AOR. Almost everybody sets this to **IDENTIFY**, which operates with the two RACINITs as described above. Other possible values are **LOCAL** (less rigor, less overhead) and **VERIFY** (more rigor, more overhead). If someone changed this value to VERIFY, it would likely increase the number of RACINITs.

The other operand **USRDELAY** tells the **AOR** how long to keep the control blocks created by these.RACINITs before the control blocks are erased (and the memory freed up). The default value is 30 minutes. Which means that if the **TOR** sends another request for some user to the same **AOR** within 30 minutes, then the **AOR** doesn't have to do the RACINIT for the **TOR**, (because he still has the control block from the earlier RACINIT). And if the same happy user sitting at a terminal types in another transaction before the 30 minutes is up, then we save yet another RACINIT, since the **AOR** doesn't have to re-do the RACINIT for the happy user.

But imagine if someone set the value of **USRDELAY** to one second. Then there would be more RACINITs.

Add an **FOR**, and the overhead increases.

This seems to be a profitable area for research. I would get the CICS sysprog (not you, I hope) to review the SMF data with you, identifying the different regions involved, which are **TOR**s etc, and the values for **ATTACHSEC** and **USRDELAY**. Make him show you the values, don't just take his word. If this doesn't work, ask him what has changed in these CICS regions to make the calls to RACF that you both see in the SMF data. (And telll us all what you learn.) I hope this leads you to a solution.

If it does, here are some conclusions:

1. Its often worthwhile to keep track of basic counts per day like number of RACINITs, number of invalid passwords, etc so you can notice when any changes start

to occur.

2. When problems arise, we should ask "what changed?". And we should shout it over the cubicle wall so all the sysprogs can hear it.

3. It's easy to blame RACF for problems caused by others. As Russ Hardgrove indicates "guilty until proven innocent". But it's been a long long time since I've seen serious performance problems caused by RACF.

4. When performance problems come up, it's useful to find out quickly whether it is caused by a problem in RACF, or by some other software calling RACF too many times. A log of the basic counts from SMF data (described in 1. above) can be very useful in this. These basic counts can be useful for a variety of other security administration functions.

New Resource Classes for MQ:

IBM has added new RACF resource classes for RACF to handle mixed case names. You'll see **MXADMIN** for **MQADMIN**, **MXQUEUE** for **MQQUEUE**, and so on. This would be a good thing to discuss with your MQ sysprog.

Better Ways to Secure Tapes:

You may have thought that turning on tape dataset protection with SETR TAPEDSN was good enough to protect tape datasets. Here are some reasons it isn't enough, followed by IBM-supplied ways to provide better protection. The ways involve a member of parmlib named DEVSUPxx, as well as your tape management software. But first the best-known problems.

Problem 1 with Tapes: If you turn on **PROTECTALL** and **TAPEDSN**, and then someone wants to process a foreign (that is, from some other data center) tape, you have to give them a way around RACF. Some people write RACF exits, others use BLP (Bypass Label Processing); still others give out the SPECIAL privilege. None of these is ideal.

Problem 2 with Tapes: Tape labels (the records on the tape that tell you the dsname of the dataset and the volser of the tape cartridge) carry only the right-most 17 characters of the dsname. So unless you store the full 44 character dsname of the tape dataset somewhere, there is a security hole. There are two places you can store the full 44 character name: the TAPEVOL resource class in RACF (which almost no one uses) OR your Tape Management Software (**TMS**).

The way to provide better protection involves four values you can set in parmlib member DEVSUPxx. They are:

- **TAPEAUTHDSN** (= YES or NO, defaults to NO)

- **TAPEAUTHF1** (= YES or NO, defaults to NO)
- **TAPEAUTHRC4** (= ALLOW or FAIL, defaults to FAIL)
- **TAPEAUTHRC8** (= FAIL or WARN, defaults to FAIL)

The latter two only apply to RACF calls caused by the first two.

TAPEAUTHDSN tells the system whether to call RACF for tape datasets (similar to SETR TAPEDSN, but doesn't use TAPEVOL records).

TAPEAUTHF1 can be used to tell your Tape Management Software to call RACF for every dataset on a cartridge instead of just the dataset you are reading. This gives extra protection against someone authorized to one dataset on a tape using that authorization to access other datasets on the same tape.

TAPEAUTHRC4 tells the system what to do if RACF is called by either TAPEAUTHDSN or TAPEAUTHF1 and RACF indicates "no dataset rule matches this dsname." This is a way to bypass PROTECTALL just for tapes

TAPEAUTHRC8 tells the system what to do if RACF is called either by TAPEAUTHDSN or TAPEAUTHF1 and RACF says to fail the request. This is like a warning mode, but just for tape datasets.

So suppose that you want to protect tape datasets using your regular dataset rules in RACF, but not using the TAPEVOL resource class. And you have **PROTECTALL** turned on. But for foreign tapes, that is, tapes from other data centers with dsnames that don't match your naming standards and don't have RACF rules, you want to allow access to anyone. You could turn off TAPEDSN (SETR NOTAPEDSN) which would de-activate the regular call to RACF for tape datasets. And then have the DEVSUPxx member of parmlib specify **TAPEAUTHDSN=YES** and **TAPEAUTHRC4=ALLOW**. Now the system will call RACF for tape datasets, but will allow any tape dataset access request that has no matching dataset rule in RACF. In effect, this turns off PROTECTALL, but just for tape datasets, which might be exactly what you want to do.

Please note also that your Tape Management Software can call RACF to provide greater functionality, and/or to ask if a user is allowed to access a specified dataset.

Of course, you still need to get a check on the full 44 character dsname, so your Tape Management Software will have to be involved. And you need to control Bypass Label Processing. And you need to take care of residual data on tapes. But now you have more tools available to you.

You should invite your Tape Management Software administrator, and whoever maintains your MVS parmlibs (perhaps your MVS sysprog) to lunch. The three of you should agree on the best approach using RACF, DEVSUPxx, and the TMS. Work out a plan to implement the three tools together, addressing all the issues with tape security. (Please see the article linked to on the last page of this issue.) Then write your decision up as policy, test it, and roll it out carefully. When the auditors come by, show them the new policy and invite them to test how well you are following it.

Or you could invite them to the lunch. Perhaps they'll pick up the tab?

RACF for z/OS 1.11 has more great features:

1. The ability to tell RACF that when a user signs on several times a day, RACF should only update the logon statistics for the first signon of each day for certain applications. The will reduce the amount of writes to the RACF database and improve performance.

2. Identity propagation that lets subsystems on the mainframe associate userids on other platforms with RACF userids You'll see this used first by CICS with networked connections.

3. RACF SMF records can be processed in XML and sent to your PC for detailed analysis.

4. Programs can now be digitally signed, making it easy to tell when a program has been changed.

5. The ability to tell RACF that when a user first tries to use USS, RACF should automatically assign the user a valid UID and GID. This should reduce the administrative effort required to create OMVS segments for users and groups by hand. This is best implemented only after you know that your USS security is rock solid.

6. Plus other system software outside of RACF will have additional security functionality.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
April 21, 2009 from about 10AM to 4PM:

Our next meeting is at DTCC in downtown Manhattan. This is a joint meeting by teleconference with the Tampa FL RUG. Attendees **must present a government issued photo ID** to enter the 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 to Hayim Sokolsky (hsokolsky@dtcc.com) with "NYRUG" or "Tampa RUG" in the subject line and your name and contact info.

❖ **You must register for the NYC meeting in advance. (Click here if reading this online)**

Please note that speakers no longer provide copies of handouts. You can print your own copies from this link: www.stuhenderson.com/XMAINTXT.HTM#handouts . 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/XMAINTXT.HTM#nyrugref .

In no predictable order, and subject to change at any time:

- Your Friend SERVAUTH or How To Protect Your IP Stack (Hayim Sokolsky)
- RACF Command Tips (Bob Hansel)
- What to Expect from an Enterprise-wide Mainframe Security Audit (David Hayes)
- More neat reporting stuff with ICETOOL, SMF, and other stuff (Mark Nelson)

The nearest subway stops are the Wall St. Station (2 and 3 lines); Bowling Green Station (4 and 5 lines); and Whitehall St Station (R and W Lines). The Staten Island Ferry is close by.

The Tampa Meeting will be at 18301 Bermuda Green Drive in Tampa. (You take I 70 North to exit 270 (the Bruce B Downs Blvd (CR 581)). Bear right at the at the end of the ramp, then at the 2nd traffic light, turn left onto Highwoods Preserve Parkway for .6 miles and turn left onto Bermuda Green Drive.
You must register for the Tampa meeting in advance. (Click here if reading this online).

For complete directions, please go to: www.stuhenderson.com/NYCRUG1.pdf Or to: www.stuhenderson.com/TampaRUG1.pdf .

HG RACF 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 "Mainframe Audit ..." classes below.)

1) HG04 **Effective RACF Administration** (**$1995**)
Feb. 24-27, 2009 in Clearwater, FL
Sept. 21-24, 2009 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($1990)**
March 31-April 3, 2009 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$510**)
June 8, 2009 in Bethesda, MD
Sept. 18, 2009 (revised) in Bethesda, MD

HG Mainframe 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 Training" classes above.)

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$1980**)
May 4-7, 2009 in Raleigh, NC
Nov. 16-19, 2009 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.) ($1590)
June 9-11, 2009 in Bethesda, MD
Sept. 15-17, 2009 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.

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** .

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 RACF User News is published two or three 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.

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/
- 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**

21 Things RACF Auditors Should Know:
This PDF file lists 21 things for auditors, including a reference on why you donMt 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 in the following article from the zJournal:

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