RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 85):

This Issue's Themes:

- Beyond Your Basic Resource Class Administration
- How Much Authority Do You Have?

Free Webinar on How to Secure Mainframe TCP/IP November 11 and 13 at 11am EST (8am PST)

NewEra Software hosts Stu Henderson's presentation of how to secure mainframe (z/OS) TCP/IP. For info, or to register for this free presentation, http://www.newera-info.com/Stu_Henderson.html

To learn about other NewEra technical webinars, please visit http://www.newera-info.com/Webcasts.html

A Friend in Europe Points Us to Two YouTube Videos

First, a video of some research on corporate passwords and common patterns used in companies: http://www.youtube.com/watch?v=qR-qRUbeKAo

Second, a video on hacking mainframes

https://www.youtube.com/watch?v=3HFiv7NvWrM

NEW YORK RUG Meeting Date

Tueday, November 25, 2014 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.** Mark your calendars now. See inside for details and new website.,

(The meeting after that will be **a Spring 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

" *Four statements lead to wisdom: I don't know. I was wrong. I'm sorry. I need help."*

--- *Armand Gamache*

Vanguard Conference

This great conference will be held twice in 2015. The spring event will take place in the eastern U.S. and the fall event will be in the western U.S. Dates and locations to be announced soon. For more information, visit www.go2vanguard.com

To subscribe to this newsletter, or for back issues:

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

Does This Describe Your Mainframe?

Many z/OS computers are front-ended by Windows or UNIX computers which talk over TCP/IP, often to the Internet. One way to find out if this is your situation is to issue the TSO command NETSTAT. This lists TCP/IP connections to your mainframe, including the programs involved. Look for CICS, DB2 (with names like xxxxDIST), TN3270 (remote logon), FTP (File Transfer Protocol), and others. If this is your situation, you will want to take care of USS and TCP/IP security, beyond dataset protection and CICS transaction security. Don't leave this to the UNIX and TCP/IP admins.

Clever Monitoring

If you want to be bored out of your mind, follow the auditor's advice to *"review the violations report every day*". If you want a fun, intellectual challenge, think how changes in volume of various things can be interesting. For example, which of these changes in number of occurrences or volume would interest you:

- Number of FTP connections per day
- Volume of data sent from your mainframe over TCP/IP
- Number of failed logon attempts
- Number of non-display operator commands issued
- Number of updates to system datasets
- Number of failed dataset accesses to production datasets
- Number of CICS transactions issued by the default userid
- Number of TCP/IP requests broken out by port number
- Number of TCP/IP requests broken out by country different from your own
- Number of printouts printed
- Number of tapes mounted
- Number of production jobs that failed because of RACF
- Number of order entry transactions processed
- Number of accounts payable transactions processed
- Number of RACF commands issued by system programmers with SPECIAL
- Number of OPERATIONS accesses other than those by storage administrators
- Number of OPERATIONS accesses by storage admnistrators
- Number of HELP transactions processed
- Number of uses of firecall userids
- Number of logons from iPhones and Androids

Think of these changes both in terms of spikes and of long-term trends. Who else might be interested (the Marketing, Compliance, Fraud, and Finance departments, the data center manager, the Network Administrator, the Systems Programming manager...)? How can you view and review the information graphically?

This Week's Exciting Contest

Develop a new and interesting z/OS based measurement, optionally describing how it might be formatted or applied. (See above.) Entries will be judged for originality, practicality, benefit, and cleverness. Winning entries will receive warm praise and adulation in a future issue. Decision of the judge is final.

Please submit entries to stu@stuhenderson.com with the subject ***RUNews Contest*** before December 31, 2014.

This Month's Featured Resource Class: DASDVOL

The **DASDVOL** resource class serves many purposes, especially for datasets on non-SMS managed disk packs. It can be used to let operators delete datasets wihout letting them read the data (eliminating the need to give them OPERATIONS).

It can also be used to give certain userids the ability to take full pack dumps and restores without granting the ability to read the data (again reducing the need for OPERATIONS). This applies both to the DFDSS and FDR disk dump and restore programs. It is also used by the ICKDSF utility program, the one which is used to format tracks, write a volume label, and create a VTOC on non-SMS managed disk packs.

DASDVOL is also used by AMASPZAP, the ZAP program which IBM has re-written to make it safe. IBM recommends protecting use of AMASPZAP with the DASDVOL resource class to protect datasets and to protect the VTOC (Volume Table of Contents) on a disk pack.

You Don't Need No Stinkin' Operations Here's the link to this classic presentation: ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/r99_dont_need_operations_for_dfdss.pdf

A Common Mistake Auditors Make About RACF

Sometimes auditors think that since you, the RACF administrator, are in charge of mainframe security, then you should be responsible for all security decisions. But you can't be. Unless you're a VTAM sysprog, you don't know whether or how to use the VTAMAPPL resource class. Unless you're a lawyer or work in the Compliance Department, you don't know what laws and regulations might address the use of Erase-On-Scratch. Frankly, you don't understand any of the business risks relating to most applications running on your mainframe. And you may not have the technical knowledge to address most of the resource classes.

So when audit findings suggest that you should be making decisions for which you have neither the knowledge nor the authority, push back. Let the auditor (and your boss) know when an audit finding is directed to the wrong person. And if the auditor can't figure out who should be catching the finding, then the auditor should be looking to address the organization's policy, not the RACF administrator. Other people approve and decide. The RACF administrator implements their decisions.

This applies to dataset rules, resource rules, option settings, granting of userids, granting of privileges (including SPECIAL, OPERATIONS, AUDITOR, protected, and RESTRICTED).

Another Step to Have 100 Percent Mainframe Security

You will want to review how you control BLP (Bypass Label Processing) for tape datasets. Anyone who is permitted to do this can bypass RACF for all tape datasets. You might consider: who has this ability now, how you control it, who approves the access, and how they make the decision. Having someone specified as the "owner/approver" for BLP, along with written approvals and annual re-certification is a good way to keep the auditors off your back.

LINUX Computers Accessing RACF Protected Datasets

New developments from IBM will make it possible for LINUX computers to access RACF protected datasets, potentially bypassing RACF. (There are three ways to have UNIX run on z systems: LINUX running straight on the z system mainframe hardware, LINUX running as a guest in a VM virtual machine (VM is an operating system that like VMware uses software to create virtual computers), and USS under z/OS.)

It is possible to have disk drives physically shared between a z/OS system and mainframe LINUX (straight on the hardware or under VM). Coming changes will make it possible for these LINUX machines to access data on z/OS disk drives. If you have LINUX in your mainframe data center now, this will be very attractive. You will want to make sure that you are in the loop if this happens, so that you can be sure the data is properly secured.

Two Ways of Looking at Security

Most RACF shops take one of these two points of view:

1. Allow everything; prevent only specified accesses.

2. Prevent everything; allow only authorized accesses.

We first saw this difference when IBM introduced PROTECTALL, the RACF switch that fails any dataset access with no matching dataset rule. Many installations resisted PROTECTALL, saying that it restricted programmers' freedom and would take too much work to implement. Several CIOs started to back PROTECTALL once they realized that it would force people to follow naming standards, which has many benefits beyond security.

Later, we saw CICS and IMS take completely different approaches: CICS fails any transaction request when RACF returns "No Matching Rule". IMS allows the access in the same situation.

And then we started using back-stopping rules (resource rules named **, which matches any name), with a UACC of either NONE or ALTER. This finessed the whole issue, and gave us control, especially useful when software vendors failed to tell us which point of view their product follows. (Of course, never use a backstopping rule for the FACILITY class, or any class which relies on the existence of a rule with a specific name.)

If you haven't done this already, you might review your resource classes, deciding for yourself which point of view you want to take for each one.

So What Resource Classes Should I Be Using?

This will very from shop to shop. Here though is a list of resource classes commonly considered essential for an effective RACF implementation:

- JESSPOOL (to control who can browse other people's printouts)
- FACILITY (for so many reasons, we can't list them all here)

- DASDVOL (see article above)
- UNIXPRIV (privileges in USS)
- TCICSTRN and GCICSTRN (unless you don't use CICS)
- VTAMAPPL (to prevent spoofing of VTAM APPLIDs)
- NODES (unless you don't have NJE)
- DIGTCERT and DIGTRING (unless you don't use digital certificates)
- APPL (to control access to various CICS and IMS regions, as well as to TSO, OMVS, and other applids)
- PROGRAM (to control who can execute certain powerful programs)
- SERVAUTH (to secure TCP/IP, FTP, TN3270, and more)
- GLOBAL (for performance)
- TSOAUTH (for TSO privileges)
- PROPCNTL (to prevent propagation of userids for CICS regions)
- OPERCMDS (to control who can execute operator commands)
- SURROGAT (to control submission of batch jobs with different userids)
- RACFVARS (to provide substitution variables for &RACLNDE and others)
- WRITER (to control who can route printouts to various printers)
- STARTED (to assign userids to started tasks)
- MQADMIN (and related classes, to secure MQ)
- DSNR (to control access to DB2)
- FSACCESS (to control access to USS file systems)
- SDSF (to secure various SDSF functions)

For each of these, you will want to verify whether you use it, whether you should be using it, who is the "owner", who approves its rules, what logging is to take place, and how to keep its rules simple enough to be effective while still easy to administer.

If You're Thinking About MLS (Multi Level Security) and SECLABELs, Read This

One RACF administrator recently learned the hard way that MLS can have unexpected side consequences. He says now that he wishes he had read all of the IBM manual "*Planning for MLS and the Common Criteria*" before jumping in. He was defining SECLABELs in RACF to be associated with columns of DB2 tables. He started to apply the SETR options to increase the rigor of SECLABEL checking. Suddenly (as in 'just after he issued the SETR"), USS signons stopped working, even though he thought he was doing nothing with SECLABELs and USS. He had never heard of pseudo-terminals before, but he has now. Here's what happened, in his own words (fortunately in an informal test environment):

"*So we're implementing MLS and I think I know a bit about RACF, so I plunge ahead, not realizing until too late that USS pseudo terminals can have SECLABELs and will inherit them if you don't pre-assign them SYSMULTI. It took me a while to realize that UNIX just thinks a terminal is just a funny type of file, and that in USS files can have SECLABELs. And the* ***chlabel*** *command can be used to assign or change a label. And the* ***ls -lM*** *command can be used to list a file's SECLABEL. But for pseudo terminals, you can't change the SECLABEL once it's assigned. Nor can you delete the pseudo term with the* ***rm*** *command and then recreate it with* ***mknod****.*

So I ended up with a few pseudo terms with SECLABELs that prevented anyone from telneting into USS, and I couldn't figure out how to get rid of them. And it was too late to assign SYSMULTI the way the book told me to.

And then I made the mistake of using ***chlabel*** *to assign a pseudo term the SECLABEL MULTISYS (when it should have been SYSMULTI). MULTISYS didn't exist as a*

*SECLABEL, but **chlabel** let me assign it anyhow. A colleague had the clever idea to create it as a SECLABEL, give it to myself.... and then get into USS and rename the pseudoterminal with the **mv** command. Then I used **chlabel** to assign SYSMULTI to all the pseudoterms (**chlabel SYSMULTI /dev/ttyp00***) and people were then able to telnet in, and I was happy.*

Until someone tried to log on with SSHD and got blocked because the pseudoterms all had SYSMULTI. So the sysprog who was the end user in this case, pointed me to the SSHD manual from IBM (page 43 of
http://www-03.ibm.com/systems/resources/fot4os02.pdf
) which says for SSHD, you need to give OMVSKERN (the userid for SSHD) the SECLABEL SYSMULTI. Which I did and it all seems to work now. (I wonder about giving a SECLABEL to this id which is used for USS itself and other things, but I followed the IBM manual and it worked.)

And then I started reading about NETACCESS statements in the TCPIP config. file and the need to put SYSMULTI or whatever on the applicable SERVAUTH rules in RACF. We don't need that stuff, but it's a possible future complication.

All of which is to say that when I activated the SECLABEL resource class in RACF for DB2, I didn't realize what else I needed to be aware of. The SECLABELs worked fine with DB2, but I didn't realize that I'd blocked all the otelnet and SSHD signons to USS. I thought I was walking into territory I understood, but when I discovered how much I didn't know about pseudoterms, I was up to my neck in quicksand. (A great IBM specialist pulled me out repeatedly.)

I hope my sharing this helps someone to avoid my mistakes in the future. Thanks for hearing me out.

PS One other point: SSHD apparently tries one pseudo term after another until he finds one that he can use. (otelnet apparently quits when the first one he tries doesn't work for SECLABELs.) This led to an SSHD blowup when he ran out of memory, an S03C4. The sysprog shared the a pile of error msgs which at first glance look like a storage problem, but really are a SECLABEL problem."

Moral: Don't jump into MLS and SECLABELs without reading that IBM manual and thinking it all through carefully.

==========

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet
November 25 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. Please see the website listed below to register.

Please note that speakers no longer provide copies of handouts. You can print your own copies from the new website listed below. Our agenda is not certain at press time. So you might check the same site for exact details as they become final.

For Complete Directions and to Register, Please Visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson. com This website has:

- Directions to the meeting and video-conferencing status
- Easy registration links
- Current version of the Agenda (subject to change)
- Links to get copies of handouts

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** (**$1995**)
March 2-5, 2015 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($2050)**
Dec. 2-5, 2014 in Bethesda, MD
Dec. 7-10, 2015 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 17, 2014 in Bethesda, MD
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**)
March 16-19, 2015 in Bethesda, MD
Sept. TBA, 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. 18-20, 2014 in Bethesda, MD
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**
- Georgia RUG at www.garug.net ..
- 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
- 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