RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 75):

This Issue's Themes:

Are simplifying life by applying common-sense comprehensive rules (such as **Walt's Rule** described below) and the wonders of the parmlibs.

Simple Steps to Report on Compliance Automatically, for Free:

Take a look at IBM's Health Checker, which automatically checks the items you want it to check, as often as you decide. You can tell it for example to verify that the UACC of APF authorized datasets is READ or less, and to tell you of any exceptions. That way, you learn about it before the auditors see it. Buy your sysprog lunch to discuss what this software can do for you. Each release of RACF has more checks you can specify.

Free Info Source on CICS Security:

New Era offers us this free book with lots of good info about CICS Security.

www.newera.com/CICS/

NEW YORK RUG Meeting Dates

Tuesday, October 20, 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,

---

NY Metro NaSPA Chapter (system programmers professional association) meets at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM. New dates are almost set now. 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 2010

Date and location are not yet determined, but you can find out as soon as it's posted at

www.go2vanguard.com/conference.php

Today's Quotation

"*Wise farmers know that only a fool gets mad at a mule.*"
– Thomas Boswell, Washington Post

A Neat Tool to Report on Your USS File Security:

You are probably familiar with IBM's Database Unload Utility that makes reporting against the RACF database as easy as pie. IBM now gives us (again for free, but on an "as-is" basis) an additional utility to make reporting of USS file permissions as easy as DBU. You can download it from:

ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/irrhfsu

See the read.me file there for more info, including:

Some examples of the data it lets you report on regarding USS files are: file permission bits, owning UID and GID, owner- and auditor-specified logging options, etc. "The **irrhfsu** utility will unload HFS file data in a manner which is complimentary to IRRDBU00. . The utility comes with sample load and table definitions for use with DB2." It can "also be used to delete ACL entries containing UIDs and GIDs which cannot be mapped to RACF user or group profiles ("orphaned" ACL entries). This ability corresponds to the ability of RACF's IRRRID00 utility to delete references to users and groups which no longer exist in the RACF database.**"** Thanks to Bruce Wells of IBM for this great tool.

Interesting Products:

We have not evaluated these products, but consider them interesting enough for you to make your own evaluation:

- EKC has a new product named "ESSF" which provides archiving and selective backup of profiles in the RACF database. Profiles may be recovered from the ESSF Dbase, or ANY valid RACF dataset on DASD available on the LPAR where the product executes. Upon Recovery/Restore of USER or GROUP profiles all the appropriate connections to/from groups/users will be automatically (re)set as required. For more info, contact EKC at www.ekcinc.com.
- IBM products and services to secure cloud computing: http://www-03.ibm.com/press/us/en/pressrelease/27269.wss
- Three security products from IBM Tivoli: http://www-01.ibm.com/software/tivoli/solutions/security/
- Tivoli Security Management for z/OS: http://www-01.ibm.com/software/tivoli/products/security-mgmt-zos/

Three Reasons to Convert from DB2 Internal Security to RACF:

1. RACF has wild cards (* and %) to protect many things with one rule
2. RACF doesn't have the "cascading revoke" "feature" of DB2 internal security.
3. DB2 release 9 will support role-based security administration with RACF.

Get More from the APPL Resource Class (Plus Performance Improvement):

We often think of using the APPL resource class to control access to CICS and IMS regions, perhaps separating production regions from test. We can also now use APPL to control access to TSO and to USS and to FTP.

To use **APPL** to control who can log onto TSO, make a rule in the APPL class with one of two names: If VTAM uses generic resources for TSO, use the **TCASGNAM** value in the **TSOKEYxx member of parmlib**. Othewise use the name **TSOxxxx** where **xxxx** is the **SMF system id defined in parmlib member SMFPRMxx**.. Also, in a member in parmlib named IKJTSOxx, specify **VERIFYAPPL(ON)**. [This is the same place you specify **PASSPHRASE(ON)** when you are ready.].

To use APPL to control who can log onto USS, use an **APPL** rule named **OMVSAPPL**.

To use APPL to control who can log onto FTP (and you may have more than one FTP), use a rule whose name is the first seven characters of the name of the FTP started task. (You can use the TSO command **NETSTAT** to see what FTPs are running on your mainframe.)

Combine these with a policy requiring every program with a sign-on screen (that is, every applid) to call RACF to check out the userid and password (instead of using hard-coded userids and passwords), and you can start to control every path into your system with RACF.

So What's the Performance Boost with APPL?

Every logon involves I/O to the RACF database, often including the "date of last signon" and other statistics. You can now tell RACF for a given APPLID when a user signs on several times a day, RACF should only update the logon statistics for the first signon of each day. To do this, specify in an APPL class rule for that APPLID. **APPLDATA('RACF-INITSTATS(DAILY)')**. If an APPL rule already has APPLDATA, see the ***"IBM RACF Security Administrator's Guide"*** to see how to include both. This will reduce the amount of writes to the RACF database and improve performance.

The Simple Way to Secure Files with Mainframe FTP (Walt's Rule):

There has been much discussion on how to secure mainframe FTP, and IBM gives us a whole slew of tools to use for this. However after the discussion dies down, one statement stands out for its simple effectiveness: *"First, secure all your datasets and resources properly*." After that, securing FTP becomes much simpler. The source of this advice is of course Walt Farrell of IBM, and some people have taken to calling this **Walt's Rule**. It makes life simpler, reduces confusion, and may apply to other aspects of RACF and life. Thanks again, Walt.

Our Latest Contest:

Walt's Rule reminds us of other great simplifying statements in history beginning with "First". Some of these are listed below. The object of our latest contest is to create a new simplifying statement that improves the quality of life and begins with the word "First".. Entries will be judged for a prize award on both cleverness and usefulness, with extra points for humor. Decision of the judges and award of prize is final. Please send your entry to stu@stuhenderson.com. The cleverest entries may receive ink in a future issue of this newsletter. Examples of similar "famous firsts":

- (Shakespeare) "First, we'll kill all the lawyers."
- (From a recipe for possum stew) "First, catch one possum."
- (physicians' prime directive): "Primum non nocere" (First, do no harm)
- (Star Fleet Prime Directive) "First, no Star Fleet personnel may interfere with the healthy development of alien life and culture"

Is There a Real Risk If I Don't Turn On ERASE-ON-SCRATCH?

Several people have questioned whether it is really possible to access sensitive disk data after a dataset has been erased, if you don't have EOS active for that dataset.

Here's what IBM says in the "***RACF System Programmer Guide***" (emphasis added):

"*The erase-on-scratch facility provides a defense against two types of attacks:*

- *It protects against an attempt to read residual data. This means that no one can allocate a new data set at the same location, open it for input, and read your data.* ***This requires no exotic tools or insider knowledge and can be done quite easily using JCL and an IBM-provided utility such as IEBGENER.***

- *It defends against an attempt to read data by acquiring physical access to a device and attempting to read its data directly." ...*

(And on performance side effects)

"Using data erasure with virtual array devices means that the storage subsystem erases data automatically without performance penalty. DFSMS checks the erase results from the RVA device. If the data was to be erased, DFSMS checks whether it was erased by the device. If it was not, DFSMS erases the data using other methods.

Two general "rules of thumb" flow from this implementation:

1. If you are using the DDSR function of IBM's extended data facility product (IXFP), specifying erase-on-scratch has minimal impact because DDSR performs the erasure in the overwhelming majority of cases.

2. If you have data for which you want to enable erase-on-scratch, allocate the data on DDSR-enabled volumes.

By following these two rules, your data can be erased by the storage subsystem in the overwhelming majority of cases. In those rare cases where the storage subsystem was not able to erase the data, DFSMS erases the data using the ERASE CCW. This is also faster than on older devices because it does not need to wait for disk rotation."

What's New for Residual Data (left on a disk pack after dataset erasure)?:

Release 1.11 of z/OS (available now) changes processing for allocation of datasets to write an EOF (End Of File) mark at the beginning of non-SMS disk datasets. (Formerly this happened just with SMS-managed datasets.) This makes it harder accidently to read sensitive residual data, although it can still be read by reading past the EOF mark. So if you don't use EOS, there is a little bit more protection than before for residual data. But it's better to use EOS for residual data, or some other protective means such as encryption.

So How Do I Tell Which Disks Datasets to Make EOS?:

This is not the RACF administrator's job. You can't know which datasets are sensitive. Instead each application's risk assessment should provide you with an indication of which datasets are sensitive and why. Use it to decide where to put EOS.

Simple Steps Now to Make MVS Security Easier and Better in the Future:

More and more, IT auditors will be asking in the course of MVS security audits: "How do you know that all the backdoors (like APF programs and User SVCS) are safe?" You can prepare good answers for the future by getting policy in place now to take advantage of the new software signing coming in z/OS 1.11. Involve your sysprogs, internal auditors, software contract administrators, and others in the discussion early on.

PARMLIB Members You Should Know:

The MVS parmlibs (parameter libraries) are the datasets where the system programmers specify MVS options, including security options. Each parmlib is a partitioned dataset, made up of mini-datasets called members. Each member has a name that tells you what sort of options it contains. If you're responsible for mainframe security, you will want to know how the options are set in at least these members:

- **AXRxx** system REXX
- **BPXPRMxx** UNIX System Services
- **COMMNDxx** automatically issued operator commands
- **DEVSUPxx** tape security options
- **EXITxx** system exits
- **HZSPRMxx** health checker
- **IEAAPFxx** APF authorized libraries
- **IEAAPP00** I/O appendages
- **IEASVCxx** user SVCs
- **IEASYSxx** starting point for MVS options
- **IEFSSNxx** functional sub-systems (like DB2 and MQ Series)
- **IKJTSOxx** TSO
- **PROGxx** APF authorized libraries, system exits, other
- **SCHEDxx** Program Properties Table (same as in DSMON)
- **SMFPRMxx** SMF options (please see Q&A in next article)

You can browse these members in ISPF. You can learn what the different options and values mean from the IBM manuals named "***MVS Initialization and Tuning Reference***" and "***MVS Initialization and Tuning Guide***".

Q & A From Our Tech Support HotLine:

Q How can I know if someone stopped SMF recording, made changes to the system without SMF records being produced, then turned SMF back on? Can MVS come up without SMF?

A. MVS can come up without SMF. See the parmlib member SMFPRMxx, the operator command HALT EOD (Z EOD), and the type 90 SMF record. Also, there should be regular checking for gaps in SMF records longer than say ten minutes. Any gap longer than that should be investigated.

NYRUG (New York RACF Users Group) and Tampa, FL RUG October 20, 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, company, phone, and email. **You must register for the NYC meeting in advance. (Click here)**

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 .

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 75 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 .

Speakers (subject to change) may include:

- **Mickie Gray** of GAO on *"RACF and Internal Control - Translating Effectively Between Both*"
- **Mark Nelson** of IBM on "*RACF update*"
- **Hayim Sokolsky** of DTCC (our host) on *"ICSF*"
- **Jeffrey Johnson** from IBM on *"Tivoli"*
- **Russ Hardgrove** of IBM on "*RACF and the Parallel SYSPLEX*"

Great Scott! Another Great Free Resource on the Internet:

Someone named Scott NLN has a great website with good, free code, including for example code to check your digital certificates and warn you if any are about to expire. Take a look at www.inherentlylame.com

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**)
Dec. 7-10, 2009 in Bethesda, MD
Feb. 23-26, 2010 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($1990)**
March 1-4, 2010 in Clearwater, FL

3) HG06 **UNIX (USS) for RACF Administrators** (**$510**)
April 15, 2010 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**)
Nov. 16-19, 2009 in Clearwater, FL
May 4-7, 2010 in Raleigh, NC

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)
April; 12-14, 2010 in Bethesda, MD

C) HG67 **Effective FISCAM Audits of Mainframes with z/OS and MVS ($1620)**
Nov. 10-12, 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 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 in the following article from the zJournal:

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