RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 83):

This Issue's Themes:

- Self Checking
- Better Security By Keeping Things Simple

RACF 2.1 Manuals Now Available

You can download them for free in pdf format at:

http://www-03.ibm.com/systems/z/os/zos/bkserv/v2r1pdf/#ICH

RACF 2.1 (and that other 2.1 software) will be available this Fall.

Barry Schrager to Discuss Security Issues December 12 at the Doubletree Hotel Times Square

Come join CSOs, auditors, and other security professionals at a technical breakfast featuring Stu Henderson and Barry Schrager (original author of ACF2) as they discuss the most common. overlooked risks in mainframe security. Contact Theresa Tama at (703) 447-1391 or theresa@xbridgesystems.com to register and learn more.

NEW YORK RUG Without Tampa RUG Meeting Dates

Tuesday, October 15, 2013 from 10AM to around 4PM.

Because of Hurricane Sandy, our meeting site has moved to IBM at 590 Madison Avenue. We will not be able to teleconference with Tampa this meeting, but hope to again in the Spring.

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 2014**)

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

"*Better to light a single candle than to curse the darkness.*"

Vanguard Conference June 23-26, 2014

This great conference will be held June 23-26, 2014 in Las Vegas, NV. Learn more at:

www.go2vanguard.com/conference.php

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

RACF Release 2.1 Controls Who Can Use Which CLASS= on JOB Card

As Mark Nelson described at our last meeting, RACF for z/OS 2.1, available this Fall, lets us control who can use which CLASSes on JOB cards. This relies of course on rules in the **JESJOBS** resource class with this format:

JOBCLASS.localnodeid.jobclass.jobname

You tell JES to call RACF for this check by creating rules in the FACILITY resource class. The existence of the FACILITY class rule named **JES.JOBCLASS.OWNER** tells JES to call RACF for job owners. The existence of the FACILITY class rule named **JES.JOBCLASS.SUBMITTER** tells JES to call RACF for job submitters.

z/OS 2.1 Supports Auto Logoff for USS Users After x Minutes of Inactivity

So we read in the release documenation. If anyone can find documentation on how to implement this, please let us know.

Why Simpler Means More Secure

The best security is often the simplest, as we learned when we implemented **PROTECTALL**. Without PROTECTALL, we could never be sure that every important dataset was protected unless we conducted a detailed review of all the datasets. With PROTECTALL, our simple starting point is that every dataset is protected by RACF.

We get similar simple assurance from features such as BATCHALLRACF and backstopping rules (RACF resource rules named ******, so they match everything).

Simple techniques like these make it easier to explain to an auditor that everything that needs to be secured is secured. And easier to know for ourselves.

With RACF 2.1, we can simplify USS file security by restricting access to a zFS file system, using a rule in the FSACCESS resource class. (The name of the FSACCESS rule is the same as the dsname of the file system dataset.) As IBM documentation describes it, "***This method supports an improved audit posture by enabling the RACF administrator to demonstrate a single point of control for restricting access to one or more file systems that might contain sensitive or personal data***."

A "single point of control" is just as valuable as not having a single point of failure.

A Comprehensive Policy Can Make Life Simpler and More Secure

Do you have a policy that every connection to your mainframes (TCP/IP or SNA) must be evaluated for security, including whether encryption is needed and how users need to identify themselves to the system?

If not, how could anyone expect you to know about all the connections and how secure each one is? How comfortable can you be about your security? To test this out, issue the TSO command **NETSTAT**. For how many of the TCP/IP connections there can you describe the security configuration?

Self Check for Health Checks

The HealthChecker is part of MVS that let us define certain checks, along with when they are to occur, how severe each one is, and what is to be done with the output. For example, you can tell the system to check once a day that IBMUSER is revoked. You can specify with this check what is to be done if IBMUSER is ever found not to be revoked: send an alert, send the results to SYSOUT, send the results to a logstream, or WTO (Write To Operator).

Here are some of the RACF checks IBM predefines for us, including some new ones with RACF 2.1:

- Is IBMUSER is revoked?
- Are any digital certificates about to expire?
- How are sensitive resources protected (parmlibs, apf libs, REXX system datasets, linklist datasets, RACF databases)?
- What AIM level is my RACF database?
- Am I no longer using IBM.DEFAULT.USER?

IBM gives us these Healthchecker checks for free. How many do you take advantage of? Which ones do you want to start using? IBM recommends that the entire baseline group of RACF resource classes be active; this is why the checks were introduced.

Wouldn’t life be simpler if you had these checks performed automatically for you, just the way you want them?

How To Define HealthChecks

To define these, you’ll use the **RACFHC** resource class

The checks are defined in a member of the MVS parmlibs named **HZSPRMxx**.. Your use the resource class XFACILIT to control who is allowed to administer health checks.

If you want to start using the health checks IBM has already defined for you, follow these steps:

1. Have your system programmer add the Health Checker started task to the system. It is almost always named **HZSPROC**.

2. Activate the **XFACILIT** resource class in RACF and define rules in it to control who can administer health checks.

3. Review the checks IBM gives us, select one to start with, and try it out in a test environmnet. Learn more from the IBM manual “***IBM Health Checker for z/OS V1R13 User's Guide***”.

Another Graceful Way to Deal With Auditors

Set up a series of HealthChecks to execute once a month or once a week, with the output going to a sysout that you don't need to print. When auditors want to know about your RACF implementation, just point them at the HealthChecks' output.

Do Started Tasks Need OPERATIONS?

Many installations routinely give many started tasks userids with the OPERATIONS privilege. This is done for one of two reasons: a belief that the started task truly needs the OPERATIONS privilege, or a belief that it is too much trouble to figure out what datasets and resources a new started task needs access to. This second approach complicates life, since you then have to stay on top of any changes to the JCL for those started tasks.

Several started tasks however do need to be protected agains RACF failures. JES and VTAM come to mind. IBM gives us a more powerful way to make sure these started tasks never fail for RACF violations: the TRUSTED attribute in their started task definitions. TRUSTED is more powerful than OPERATIONS since it applies without exception to all datasets and to all resource classes.

IBM gives us a list of which started tasks truly need TRUSTED. You can find this in the IBM manual "***MVS Initialization and Tuning Reference***", in the section headed ***Assigning the RACF TRUSTED attribute"***. Other started tasks may also need TRUSTED, depending upon what the vendor documentation says, and depending on your own risk assessment.

Note that a started task marked TRUSTED is also automatically treated as a SUPERUSER (UID of 0) in USS.

So What's the Real Risk If I Do Give a Lot of Started Tasks OPERATIONS?

Some people say that if you give OPERATIONS to a started task, there is little risk, since it's a fixed task, and not a person. However, this complicates life by introducing two additional risks:

a. Someone might modify the JCL for the started task, inserting a new job step for some rogue program.

b. If the started task is, for example, a CICS region, then someone could add a transaction to it that submits a batch job. If the JOB card doesn't specify USER=, then the job inherits the userid of the region, which has OPERATIONS. (Note that the TRUSTED privilege is not inherited by batch jobs, only OPERATIONS.)

So life is simpler if you don't give OPERATIONS to started tasks that don't truly need it, as indicated by vendor documentation or your own risk assessment.

To keep life simple, you may want to avoid giving started tasks the OPERATIONS privilege. Use TRUSTED, and only for started tasks that truly need it.

Why Started Tasks for CICS Region Should Not Be Marked TRUSTED

When a CICS transaction connects to MQ Series to put and get information to and from a queue, MQ decides when to call RACF. For example, MQ can decide to call RACF when the transaction asks MQ to open a queue,.

MQ will decide not to call RACF at all for CICS transactions from a given region if the userid of the region has UPDATE or higher permission to a RACF rule named **ssid.RESLEVEL** in the MQADMIN resource class. The region will have this permission if it is a started task marked TRUSTED. So if a CICS region is marked TRUSTED, then any transaction in it that uses MQ will have no RACF calls when it accesses MQ resources.

Interesting Products While we do not generally endorse products, we do mention ones that you might want to evaluate for yourself. Here are two:

ReACT – Enterprise Self-Service Password Reset. In just 4 easy steps, users can reset & synchronize passwords across the entire enterprise, including RACF, Top Secret, AD, Novell, UNIX, Linux, Oracle, SQL, Google Apps, Live@Edu/Office365, SAP, AdvantX, Datatel and more. Additionally, ActiveX scripting allows ReACT to tie into custom applications. ReACT eliminates password reset related calls to the Help Desk and provides leading-edge features such as multi-factor authentication [image recognition, SMS, email, AD, challenge questions] and an Administrative Dashboard. For more information: www.aspg.com .

SDS now supports and develops **McAfee's EeBusiness Server suite** of products, which provide industrial-strength, automated Encryption and permits IT administrators and developers to embed encryption, decryption, digital signing, and authentication within applications or batch processes. It incorporates the industry's strongest encryption algorithms, including Triple-DES, CAST, IDEA, Twofish, AES and Blowfish algorithms. Contact Deb Hodson, Software Diversified Services, 1322 81st Ave. NE, Minneapolis, MN 55432 Tel: 763-571-9000 Email: info@sdsusa.com

How to Figure Out How Someone Learned All Your RACF Passwords

If some hacker learned just one person's passwords, you might consider the threat to be minimal. But if you discover that some hacker learned all of the passwords of all the users in your RACF database, the hacker almost certainly had READ access to some copy of your RACF database. To find out how, you will want to identify all the copies of the RACF database and its backups, including full disk pack dumps to tape, and copies sent to the disaster recovery site. You'll then want to discover who had READ access to any of these copies by any means, including: the OPERATIONS privilege, started tasks marked TRUSTED or PRIVILEGED, the GLOBAL ACCESS table, firecall ids, accesses over shared DASD, and access to tape datasets with BLP. (If you recently re-allocated your RACF database, did you write zeroes over or otherwise obliterate the old copy?)

An interesting exercise might be to count how many people have such access now. Remember that anyone with READ access to a copy of your RACF database can learn all the passwords with a password cracker program, regardless of what encryption is used. Life is simpler if you know, and can demonstrate, that no one has READ access to any copy of the RACF databases.

NYRUG (New York RACF Users Group) Without Tampa, FL RUG October 15, 2013 from about 10AM to 4PM:

Our next meeting is at IBM, 590 Madison Avenue in Manhattan. This is usually a joint meeting by teleconference with the Tampa FL RUG. We will not be able to include the Tampa Bay RUG this meeting, but hope to teleconference with them in the Spring.

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

New Format for NYRUG and Tampa Bay RUG Meetings

We are enhancing the RUG format as follows:

- The first half hour (the Early 30) will be dedicated to a variety of very brief discussions, including topics for the Five Minute Madness (see below), update on the latest features of RACF, RUG meeting logistics, Stump the Experts, and others. The next hour will be a tutorial for those who would like a re-cap on some basic RACF topic.

- Right after lunch we will have a "Five Minute Madness" where anyone can speak for five minutes on any reasonable, interesting, non-marketing, usually security-related topic. (To speak during the 5MM, you will need to suggest the topic and have it approved before the meeting. Email your suggestions to stu@stuhenderson.com, specifying the Subject as 5MM. We will give wide latitude in approving topics, but the five minute limit will be enforced.) Topics could be short descriptions of clever solutions to specific problems or requests for information or surveys of members or anything you want. We will list the topics on the website as they become approved.

- The last session will be a discussion of proposed RACF requirements to pass onto IBM. Please use the form on the website to make your suggestions. Please note that proposed requirements must be made available to us by 9AM the Monday before the meeting. See the form provided on the website. There is a limit of three proposals per organization.

- The rest of the meeting will be familiar format with a series of hour or so long presentations, some technical and some addressing RACF administration.

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**)
Dec. 2-5, 2013 in Bethesda, MD
Feb. 25-28, 2014 in Clearwater, FL

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

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 17, 2014 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, and DB2** (**$2100**)
Oct. 29 - Nov. 1, 2013 in Chicago, IL
March 3-6, 2014 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)
Nov. 18-20, 2014 in Bethesda, MD

C) HG76 **How to Audit TCP/IP Security (\$575)**
Dec. 1, 2014 in Bethesda, MD

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

.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, 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 at www.stuhenderson.com/XMANETXT.HTM.

To Get a Free Subscription to the RACF User News Phone Stu at (301) 229-7187 with your request, leaving your name, email address or 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 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 software and tape management software