RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 84):

This Issue's Themes:

- Checking Up the Things That Need Checking
- Prepping for 2.1

Chicago RUG Meets Thursday, March 20

For info, contact Pat Diya at email: patricia.diya@acxiom.com OR phone (630) 944-5142

YouTube Video of Mainframes in the Movies

Check it out at

http://www.youtube.com/watch?v=Hcywf9mwF5U

What Fifty Year Anniversary May Be More Important Than the Beatles Arrival in America?

Answer: the Mainframe turns 50 this year. Happy Birthday!

NEW YORK RUG and Tampa RUG Meeting Date

Wednesday, April 23rd, 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 Fall 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

"*The technical part is easy now. Figuring out how to provide adequate security without adequate authority and without adequate budget is hard.*"
--- Anonymous RACF Administrator

Vanguard Conference June 23-27

This great conference will be held June 23-27, 2014 in Las Vegas, NV. Learn more at: www.go2vsc.com

_____

Special Discount to Our Readers

When registering for the Vanguard Conference, use the code IND to get a $200 discount. Vanguard customers should contact their account manager before registering.

Two Basic Concepts for TCP/IP

To understand TCP/IP (and to secure it), you need to understand these:

- an **IP address** is used to route a TCP/IP message to the correct computer. An IP address (often made up of four numbers separated by dots) corresponds usually to one computer. It also corresponds to the part of a DNS name that ends in .com or similar. You will want to learn what IP addresses, and what DNS names map to your mainframes.

- a **Port Number** corresponds to a single application, such as FTP, email, telnet, TN3270, CICS, DB2, or MQ Series. Once a TCP/IP message arrives at your computer (routed by means of the IP address), TCP/IP on the computer reads the port number of the message to determine which application to hand the message to. The applications are often started tasks with RACF userids. You will want to know what ports are active on your mainframes, and what ports are protected. Use the TSO command N**ETSTAT** to find out.

To know that your mainframe is protected from TCP/IP attacks (including attacks over the Internet), you can specify options in the TCP/IP configuration files to block ports, and to provide encryption when passwords or other sensitive data are sent over the network. You can use the Policy Agent started task to provide firewall-like protection of your mainframe. You can also use the SERVAUTH resource class in RACF. You should not rely solely on Windows or UNIX firewalls between your mainframe and the Internet.

At a minimum, you want to ensure that only authorized users can modify the programs, JCL, and configuration files used by TCP/IP and its applications.

If this seems complicated, you still need to address it. A good idea might be to find out who administers TCP/IP on your mainframes and invite him or her to lunch. Your mainframe will not have effective TCP/IP security unless the two of you work together.

Neat New Features in ISPF to Address Mainframe Security (Thanks to Mark Nelson)

At the last NYRUG meeting, Mark described a powerful tool named ISRDDN which can be used in TSO to:

- Examine the datasets allocated to a DD name
- Browse storage that is accessible to non-authorized callers
- Identify the 'fetch location' for a module loaded by the user
- Find the data sets which contained a specific member
- Identify I/O errors caused by mixed record format allocations
- Find who is allocated specific data sets
- Identify member names or LPA load modules are duplicated in the user's current allocations
- Find empty datasets in data set concatenations

This is a powerful tool that you can use to review MVS security and for many other purposes. You can learn more from his handout at:

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2013_10_isrddn.pdf

Free Webinar Repeated by Popular Demand

"***Twelve Most Overlooked Mainframe Security Exposures and Lessons from an Actual Mainframe Break-In Over the Internet***"
March 18 11-noon Eastern Daylight Time and
March 20 11-noon Eastern Daylight Time

Click here to learn more or to register: http://www.newera-info.com/Webcasts.html

New Features with z/OS and RACF 2.1

(Thanks to Julie Bergh of IBM. See the handout from her presentation at the last NYRUG meeting at http://www.stuhenderson.com/Handouts/z_OS_2.1_Security_Updates.pdf)

- **(Thanks to Alexander Riedel who told us about this.)** You can now have Auto Logoff for USS users after x minute of inactivity. As Alexander has pointed out, the IBM manuals "***MVS System Management Facility***" and ***"MVS Initialization and Tuning Reference***" tell us how to do that, using the **SMFPRMxx** member of parmlib. Note that the Job Wait Time specified there causes a terminal to be auto-logged-off after a specified number of minutes of inactivity. With this new feature, you can extend this capability to USS logons. See the descriptions in those manuals of **PWT**, **_BPXK_TIMEOUT** and **TMOUT** variables.

- New Healthchecks, and the Healthchecker gets started by default. IBM recommends that the entire baseline of RACF resource checks be active.

- RACF control over use of **CLASS=** on JOB card

- You can now restrict access to USS file systems using the resource class **FSACCESS**. (In USS, a file system is a disk data set which is made part of the directory tree. Say you want to port a UNIX application from some UNIX computer to USS. You would copy the file system (directory tree) from that computer to be an MVS dataset that you would make available to USS. You would then use the USS command mount to tell USS to plug the top of that new directory tree into some place (called a mount point) in the USS directory tree, so that the two directory trees are treated as one. If you wanted to restrict who could access the part of the merged directory tree represented by the new file system, you would make a rule in the resource class **FSACCESS.** The name of the rule would be the dsname of the MVS dataset where you copied the file system from the other computer.)

- RACF now supports new caching for RACF rules for DB2. (When you use RACF instead of DB2 internal security (a very good thing to do), then DB2 caches or saves the results of each call to RACF. If you change the rule in RACF, you haven't changed the cached copy, and a SETR REFRESH is not sufficient to make the change take effect. You have to tell DB2 to purge his cache of the saved copy kept there. This new feature use ENF (Event Notification Facility) to do this.

IBM manuals for 2.1 are available for free in pdf format at:
http://www-03.ibm.com/systems/z/os/zos/bkserv/v2r1pdf/#ICH

How to Think About USS Security

USS (UNIX System Services) is of course UNIX on the mainframe under the control of MVS and RACF. If you are a RACF administrator, you cannot ignore USS security, since it both affects the quality of your RACF implemenation and depends upon it. Here are some suggested minimum guidelines you need to consider for USS security:

- Be sure that **FACILITY** class rules named **BPX.SUPERUSER**, **BPX.SERVER**, and **BPX.DAEMON** are all defined, and with a **UACC** of **NONE**.
- Remove all instances of root (aka Superuser or UID(0) userids which represent people. You can identify ids with root by issuing
  SEARCH CLASS(USER) UID(0)
- Use a rule named **OMVSAPPL** in the **APPL** resource class to control who can access USS.

IBM Statement of Direction Describes Coming Encryption Advances and More

In the recent announcement letter for System z, IBM states that:

"Enhanced RACF® password encryption algorithm: In the future, an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible."

Note that ACF2 and TopSecret already offer password encryption with AES (which is considered more rigorous than DES). Note also as described in Issues 82 and 83 of this newsletter that the difference between DES and AES is trivial so long as you prevent improper READ access to the RACF database and its backups.

The Statement of Direction is available at:
http://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/9/897/ENUS114-009/index.html&lang=en&request_locale=en

How to Prevent Users from Seeing Filenames They Don't Have Access To

IBM calls this ***name-hiding***. You can do this with the SETR option **MLNAMES**, which works even if you don't use security labels. As always with any new feature, before installing consider carefully what are the performance effects. Coordinate with your sysprog to test thoroughly.

Why would you want this? Any time that the spelling of your DSNAMEs or USS filenames contain sensitive information. For example, if your file or directory names include the names of your clients, and you perform some sensitive function for them, they may not want their names exposed to every programmer in your shop.

How to Be Sure You're Current on z/OS Software Releases and Service

IBM's portal is at http://www.ibm.com/systems/z/advantages/security/integrity.html . This is one worth spending some time exploring.

Make Sure RACF Performance Is As Good As You Want It

It is very rare now for RACF to cause any performance problems. But it's a good idea every year or so to make sure that you are doing everything you can make sure that RACF isn't slowing your system down. Most of these performance features involve locking RACF rules in memory to reduce the number of reads and writes to the RACF database. Here are some steps to discuss with your performance tuning sysprog:

- Consider RACLISTing every resource class that supports it.
- Ask your sysprog to monitor I/Os to the RACF database and its backup to manage any delays there.
- Make sure the RACF database and its backup are on different disk packs, with separate I/O paths.
- Move the RACF database and its backup to faster disk packs or to disk packs not containing any other high activity datasets.
- Use GLOBAL rules to reduce reads and writes to the RACF database.
- Use the IRRUT200 utility to analyze the RACF database. Make sure the index structure has no problems, and that internal space allocation has no conflicts. Evaluate how much "churning" there is (wasted index record space, similar to control interval splits in VSAM). If need be, use the IRRUT400 utility to compress the RACF database and its backup.
- Simplify dataset and resource rules with RBAC (Role Based Access Control), giving permission to groups and never to userids, and having no more than 4 or 5 dataset rules per production application.
- Simplify any dataset or access rules with more than four or five entries in the permit list.
- Ensure that no CICS transaction is defined more than once in both TCICSTRN and GCICSTRN.

Interesting Products Column

We generally leave it to you to make your own software evaluations, but occasionally mention ones we think you might find worth taking a look at.

- ***WDS - Free, Even More Powerful Network Management Utilities***,
  The ZEN Rexx Function Pack provides extensions to standard Rexx through which you can communicate directly with ZEN. The Command Interface enables you to issue commands from your ZEN Rexx programs and get any responses back. Further details from Graham Storey, Vice President Marketing William Data Systems, Email: graham.storey@willdata.com Office: 703 674 2200

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet April 23 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

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**)
October 27-30, 2014 in Raleigh, NC
March 2-5, 2015 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, DB2, and MQ Series Security** (**$2300**)
Sept. 29-Oct. 2, 2014 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

C) HG76 **How to Audit TCP/IP Security ($575)**
Dec. 1, 2014 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:
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 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