RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 89):

This Issue's Themes:

- You need to clarify who makes which security decisions
- You need to know a bit about USS Security

STIG Now Recommends EOS for All Datasets

The US government STIG (Security Technical Informaiton Guide) for RACF Version 6 Release 25 specifies that "***The ERASE ALL SETROPTS value must be set to ERASE(ALL) on all systems***." This is in contrast to earlier releases which required EOS only for selected datasets on non-classified systems.

(Note that the G in STIG stands for "Guide", not for "Law". So let's base our decisions on reducing risk and practicality.) Speaking of practicality, this change in the STIG may be partly due to performance improvements, as noted by Cheryl Watson and Frank Kyne. They show with hard measurements that EOS is much, much faster with z/OS 2.1 than z/OS 1.13. See details in the last three slides of www.stuhenderson.com/Handouts/DontKnow.pdf .

They comment that the measurements show such stunning performance improvements that any installation not using EOS should re-visit the issue, once you get to z/OS 2.1.

NEW YORK RUG Meeting Date

April 20, 2015 from 10AM to around 4PM.
at IBM in Tampa and NYC.

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.** See inside for details.

(The meeting after that will be **a Fall date to be determined in 2016**)

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

"*There's no PTF for stupid" — mainframe developer*

Vanguard Conference

We expect to have information about this great conference for 2016 shortly. Please watch this space.

For more details, visit www.go2vsc.com
For more information, please contact glory.wade@go2vanguard.com .

To subscribe to this newsletter, or for back issues:

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

Does Your Data Center Look Like This?

It's become almost a cliche: a mainframe holding and processing all the important data, surrounded by Windows and UNIX servers which face the Internet and support e-commerce with customers. The Windows and UNIX servers are not big or fast enough to process all the data and transactions, so they turn to the mainframe to do so. This raises two interesting questions:

First, does anyone understand the entire picture and its information security? This means having a map of the servers, the network, the firewalls, the mainframe, and all the security checks. This means being able to trace what happens and what paths data flows over, when a customer starts a transaction over the Internet, through the distributed servers, to the mainframe, and back. This means being able to demonstrate that there is adequate protection against any expected type of attack. If we don't have this, then it makes sense to start getting people talking to each other, at least to get an understanding of where we are. It's difficult to say that "controls are reasonably effective" if we don't have this understanding. What managers need to be involved to help develop this understanding?

Second, Since the mainframe supports UNIX (USS), TCP/IP, and all the standard daemons like FTP and http, what would be the effect of moving all the software on the Windows and UNIX servers onto the mainframe? If it's all standard stuff, this should not be difficult. There would be savings in software licensing fees, hardware costs and administrative overhead. There would be improvements in response time, reliability, scalability, flexibility, and security. If your CIO wants to improve her budget, this would be something worth investigating.

CYA (Career Yearly Assessment)

It makes sense to check your career progress, along with your organization's information security progress, just to verify where you stand, and what steps you want to take next. Part of this is the recognizing that if there is a problem with some aspect of mainframe security, people will assume that it is the fault of the RACF administrator, unless it is very clear that someone else is responsible. For example, a RACF administrator likely does not have the knowledge to know which powerful programs should be controlled by RACF. Ideally, policy will state that system programmers, who do have the knowledge, will provide direction to the RACF administrator. In the suggestions below, the phrase "***Clarify policy***" is shorthand for getting policy to specify who, other than the RACF administrator, is responsible for decision making.

We presume that you want to know more about mainframe security beyond RACF, and that you want to network professionally with mainframe technical specialists. You want to understand technical security issues as much as possible, both to satisfy your curiosity and to be prepared to deal with auditors. You want to work with technical specialists to be prepared to respond to any audit findings.

With that in mind, here are some aspects of mainframe security you might want to address, along with straightforward questions you can ask to determine where you stand, while starting to network with people you want to know. You'll have to figure out who to talk to, in order to get answers, but that's the real point anyhow. Your management should provide you an expense account to buy the technicians lunch, a worthwhile investment.

MVS Security is based on a hardware control called Supervisor State. You don't need to be a hardware expert. Just understand that any program running with Supervisor State can bypass all the security (including RACF) on the system. System programmers can give a program Supervisor State by updating certain key system datasets. You, the RACF administrator, don't have the knowledge to decide which users should have UPDATE ability in RACF to those datasets. **What you can do:** Ask system programmers what programs need to be protected and who should be permitted to execute them. Ask them to specify who should be able to execute operator commands (both MVS and JES). Work with system programmers to make sure that all started task userids are protected in RACF (that is, have no password or password phrase). Work with system programmers to specify which started tasks should be marked TRUSTED in RACF. Ask system programmers what reports they would like to get from RACF and from RACF-related SMF records. ***Clarify policy*** for key system datasets and for FACILITY resource class rules whose names begin **CSV**, as well as for the PROGRAM and OPERCMDS classes.

DB2 Security is based on DB2's internal structure of tables and databases. Security is either internal (based on DB2 security tables) or external (based on RACF resource rules). Most people consider the external security to be preferable. However the conversion from internal security to RACF security for DB2 is a major and expensive project.

Each DB2 sub-system (aka "instance" or "copy") is identified by a four character sub-system identifier, such as **DB2T** for test and **DB2P** for production. With external security, the names of all the RACF rules begin with the sub-system identifier. (In some instances the RACF resource class name includes the sub-system identifier instead.)

Each DB2 sub-system has a configuration file named DSNZPARM where all the options are specified, including the security options. Security options include TCPALVER and SECUREPORT. IBM recommends that TCPALVER be set to NO, which means that users connecting to that DB2 over TCP/IP are required to prove their identity, for example by providing a password. SECUREPORT specifies that TCP/IP connections to that DB2 are to be sent over an encrypted connection. Of course if passwords are being sent over TCP/IP, encryption is recommended.

You can learn more about security options in DSNZPARM at: http://www.stuhenderson.com/NewDB2.pdf .

Whether DB2 security is internal or external, access to DB2 is always controlled by calls to RACF in the resource class named DSNR. (Humor note: **DSN** is IBM's abbreviation for DB2. If you thought it was short for **dsname**, just ask any DBA.) Names of rules in this class always begin with the sub-system identifier. The second part of the rule name indicates whether it is controlling

access from: TSO and batch, CICS, IMS, or TCP/IP. **What you can do:** Learn the names of all the DB2 sub-systems and whether they use internal or external security. List the rules in the DSNR resource class (RL DSNR * ALL). Determine the settings for TCPALVER and SECUREPORT. ***Clarify policy*** for DSNR and other DB2 related resource classes.

MQ Security is based first of all on a series of switches which tell MQ whether to call RACF or not. Each instance of MQ (for example, MQ Test and MQ Production) is identified by a four character sub-system identifier, for example **MQ01**. Each RACF resource rule for MQ has a name that begins with that system identifier. MQ calls RACF only for events (such as opening a queue or issuing a command) for which the switch is set to YES.

One special rule can override all of the MQ calls to RACF. It is named xxxx.RESLEVEL in the MQADMIN resource class (where xxxx is the sub-system identifier, making our example be MQ01.RESLEVEL). If a user is permitted to that rule with elevated privileges such as UPDATE or CONTROL, MQ doesn't bother to call RACF for that user. **What you can do:** Learn the names of the MQ sub-systems, and how the switches are set for each. ***Clarify policy*** for MQ related resource classes, especially the RESLEVEL rules.

USS Security (Please see following article on basics of USS file security.) **What you can do:** Issue the RACF command **SEARCH CLASS(USER) UID(0)** to learn which users have that privilege. ***Clarify policy*** for UNIXPRIV, FSACCESS, and FSEXEC resource rules, and for UID(0), as well as for FACILITY rules whose names begin BPX, and the APPL resource rule named OMVSAPPL.

TCP/IP Security is based on IP addresses and port numbers. (IP addresses are used to route messages to the correct computer. Port numbers correspond to the applications or daemon programs which run on that computer. TCP/IP uses the IP address in each message to route it to the correct computer. Once a message arrives at a given computer, TCP uses the port number in the message to hand the message to the correct application.) For example, port numbers 20 and 21 are often used for the FTP (File Transfer Protocol) application.) Many TCP/IP functions can be protected by means of RACF rules in the SERVAUTH resource class. The TCP/IP configuration files specify several security functions, including blocking of ports and encryption. IBM gives us a free firewall program named Policy Agent or PAGENT. This can provide security functions such as intrusion detection, encryption, packet filtering, blocking of ports, and IPSEC. **What you can do:** ***Clarify policy*** for SERVAUTH resource class rules and for Policy Agent. Determine whether Policy Agent is in use. Issue the TSO command NETSTAT to see which programs on your mainframe are communicating over the network. This will also tell you whether PAGENT is active. Ask someone to walk you through the security options set in the TCP/IP configuration files.

Basics of USS File Security

USS (UNIX System Services) is a full-fledged, standard version of UNIX which is integrated with MVS and RACF security. One key aspect of USS security is file access control. Here are some basics for RACF administrators:

1. Each file system is a VSAM file on the outside, but a directory tree (like the directory tree on your Windows hard drive) on the inside. As in your Windows hard drive, the top of the directory tree is a directory named */*.

2. Each VSAM file which is a file system should be protected by a dataset rule. Each can also be protected by a resource rule in the **FSACCESS** resource class and by a rule in the **FSEXEC** resource class.

3. As with other versions of UNIX, users are identified by a number called a UID. If the UID is zero (called “root” or “superuser”), then that user has total access to every USS file. RACF userids are mapped to USS UIDs by storing the UID for each user in the OMVS segment of the RACF user profile. (OMVS was the original name of USS.)

4. As with other versions of UNIX, groups of users are identified by a number called a GID. RACF groups are mapped to USS GIDs by storing the GID of each group in the OMVS segement of the RACF group profile.

5. So you give someone a USS identity by giving her a RACF userid with a UNIX UID in the OMVS segment of the RACF user profile. You want to avoid accidental assignment of the same UID to two or more users. You want to restrict UID zero to the least number of users required. (Some people believe that no person requires permanent UID(0) since you can use FACILITY class rules to let specified users give themselves UID(0) on an as-needed basis.)

6. Each UNIX file is part of the directory tree inside the VSAM file described in 1. above. Each UNIX file is protected by a FSP or File Security Packet. There is one FSP for each UNIX file. It is comparable to a dataset rule in RACF. Each FSP has three sets of permissions: one for the owning UID, one for the owning GID, and one for everyone else (“the world”). Each of these three sets of permissions has three on/off switches for: READ permission, WRITE permission, and EXECUTE permission. These three on/off switches are represented as RWX.

   So a listing of the FSP will show: the RWX switches for the owning UID, the RWX switches for the owning GID, and the RWX switches for the world, followed by the owning UID, the owning GID, and more information.

7. To list the FSP for a UNIX file, issue the UNIX command:
   ls -l filename For example: **ls -l /u/stu/mydata.txt**

   The result for example if the owning UID is GEORGE and the owning GID is GROUPA, might look like:

   -rwxr---x 9 GEORGE GROUPA 26 Jan 3 12:59 mydata.txt

   (The first dash says that this is a file. The following **rwx** says that RACF userid GEORGE (the owning UID) can read, write, and execute it. The next **r–** says

that the RACF group GROUPA can read, but not write or execute it. The next **--x** says that the rest of the world can only execute it. The file is 26 bytes long.)

7. To access a file, you need permission from the file's FSP. You also need Execute permission on each directory in the path to the file, based on the FSP for each directory. In our example, you would need Execute on /, on /u, and on /u/stu.

8. Certain RACF resource rules in the **FACILITY** class are important for USS security. They all have names beginning with BPX. . (BPX is IBM's abbreviation for USS, which used to be called OMVS.) The **UNIXPRIV** resource class in RACF is used to control certain other privileges in USS.

Free Sources of Useful Guidance for InfoSec

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository
- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53
- Handouts from previous meetings of the NYRUG: http://www.nyrug.stuhenderson.com/handouts.HTM
- NewEra hosts free webinars on a variety of mainframe topics. You can see the schedule, and get handouts from previous sessions, at: http://www.newera-info.com/zwebs.html

Three Calls for Info Sharing

RACF user groups are looking for your input. Help them out by sharing your thoughts on these topics:

1. The NYRUG is always looking for real-life user experiences. For example, at the next meeting, we plan on having an administrator and system programmer who has successfully implemented KDFAES password encryption share his experiences. If you have pulled off something cool in RACF, or just managed to deal with some difficult aspect of RACF, you might want to share with others at a RUG meeting. Contact Stu at stu@stuhenderson.com for more details.

2. RUG managers want to provide you with information that is useful to you. You can assist us in selecting presentation topics for future meetings, please respond to the following survey by Friday, February 5th. Please submit one response for your entire organization. http://sgiz.mobi/s3/RUG-Member-Survey-2016 Please do not submit to this survey unless you attend meetings of a RACF User Group.

3. We can all benefit from improvements in RACF log reporting based on SMF data. If you have neat techniques for reducing SMF data for RACF administration and would like to share them with the world, please contact Stu at stu@stuhenderson.com.

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet April 20, 2015 from about 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa, 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.
For Complete Directions, to get copies of handouts and to register, please visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.

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** (**$2195**)
March 1-4, 2016 in Clearwater, FL
December 6-9, 2016 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
Dec. 12-15, 2016 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 9, 2016 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**)
May 10-13, 2016 in Raleigh, NC
September 19-22, 2016 in Chicago

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. 15-17, 2016 in Bethesda, MD

C) HG76 **How to Audit UNIX and Windows Security ($2200)**
October 24-27, 2016 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:

- 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