RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 95):

This Issue's Themes:

- New System Software, New Security Features
- IT governance
- Audit findings

Free Webinars: NewEra sponsors great webinars each month on topics like:

- The ABC's of z/OS Integrity
- Preparing for Your Next Upgrade of z/OS
- Let's Build a z Environment

See the schedule at:
www.newera-info.com/Month.html

If you miss these, you can get recordings and copies of handouts at
www.newera-info.com/Presenters.html

Where to Get IBM z/OS Manuals

Here's a link that works:

https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosInternetLibrary?OpenDocument

Where to get info on new software

(From the RUG handouts page, after May 15)

http://www.nyrug.stuhenderson.com/handouts.HTM

NEW YORK RUG Meeting Dates, Now Expanded to Dallas, Raleigh, as well as Tampa, May 15, 2019 from 10AM to near 4PM *at IBM in Dallas, Raleigh, 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).** See inside for details. (The meeting after that will be **in the Fall of 2019**)

If you want reminders of upcoming RUG meetings, please click RUG Reminders to receive one email reminder before each meeting (two per year).

Please Note the New Website for the NYRUG and TBRUG and Raleigh and Dallas RUGs: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG and Raleigh and Dallas RUGs at www.nyrug.stuhenderson.com

---

Today's Quotation

"*You are the place where I stand when my feet are sore*"

— Irish definition of a friend

Vanguard Conference

The Vanguard Security Conference is in Charlotte, NC September 30-October 3, 2019. Visit www.go2vsc.com for more details.

To subscribe to this newsletter, or for back issues:

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

==========

New z/OS Release 2.4 with New RACF Release 2.4

In September, 2019, IBM is making available z/OS 2.4, including RACF for z/OS 2.4. Here is their description of some of the new security features:

Improved PassTicket security

Today, a PassTicket key can either be masked and stored in the RACF database, or encrypted, and stored in ICSF. Enhancements in RACF provide new capabilities to facilitate the use of encryption with ICSF as the key store for PassTicket keys in order to provide enhanced PassTicket keys security and protection against cyber attacks. The new functions include:

Command and programming interfaces to report on the method of protection for PassTicket keys, and, for encrypted keys, the ICSF key label name.

A function to convert masked keys to encrypted keys without needing to change the keys.

The ability to use pre-existing keys in ICSF for application PassTickets.

Enhanced RACF usability and threat detection

RACF is enhanced to enable clients to extend the "RACF schema" to store securityrelevant information within the RACF database, where existing reporting tools and programming interfaces can be used to manage and retrieve the data.

RACF users can add custom fields to RACF general resource and DATASET class profiles in a consistent fashion with the existing ability for user and group profiles.

For all profile types, the ability to validate the value of a field using a System REXX program is also provided.

RACF users are allowed to retrieve DATASET class profile fields using the R_admin callable service (IRRSEQ00) and the IRRXUTIL rexx interface.

RACF's IRRXUTIL rexx interface is enhanced to allow retrieval of a general resource class definition from either the static or dynamic Class Descriptor Table (CDT). The current SETROPTS settings for the class can be optionally requested.

RACF also can detect changes to a user's security environment, including change in privileges.

A new message is issued when such a modification is detected.

Exceptions can be defined for trusted applications in order to suppress the message for users of such an application.

New CICS Release 5.5 with New Security Features

- The new CICS offers these security enhancements:
- A new surrogate security check restricts the ability of users to submit jobs using the EXEC CICS SPOOLWRITE command. Performs surrogate user checking to verify if the user is authorized to submit a job with the USER ID specified on the job card.
-
- Group on VERIFY to improve use of passtickets
-
- User terminal access restricted when using a default user ID
-
- Increased minimum Transport Layer Security (TLS) level
- User ID changes for use with Kerberos service principle for a CICS region.

Another Look at Erase-On-Scratch Performance

EOS (Erase-On-Scratch) is a RACF feature that protects senstive data by obliterating the data in a disk dataset when the dataset is erased . Without this feature, the data is at risk of being copied by unauthorized parties the next time that part of the disk drive is allocated to someone else's dataset. Some shops have held back from implementing EOS because of performance problems from the past.

Here's an update on performance improvements with recent releases of z/OS:

- EOS has been improved so that it immediately frees up the channel and the control unit (keeping only the specific disk drive busy) while the data is being obliterated
- Starting with z/OS v2.1, up to 255 tracks can be obliterated with one CCW command
- With z/OS v2.2, up to 12,240 tracks can be obliterated with one command

In addition, the latest versions of the NIST STIGs (Security Technical Information Guides) nowcall for EOS.

So if you've been holding off from EOS for performance reasons, you might want to re-test whether it slows the system down to any noticeable degree. Of course, EOS may not be needed for datasets that you will soon be protecting with Pervasive Encryption. Your organization will need to make that decision.

And to keep the auditors at bay, you might want to document your decision, "We are not implementing EOS because the attached testing results demonstrate that the performance effects would make our system inoperable." Or "We are implementing EOS only on datasets for which our risk assessment indicates the need, and which are not capable of protection by means of Pervasive Encryption. We reserve the right to de-activate EOS for datasets where EOS causes serious performance problems...."

(Thanks to Mark Nelson and the RACF-L for the detailed numbers above.)

Projecting History Into the Future ("Give me two data points and I can show you a trend.")

In the beginning, a system programmer installed RACF and defined some users and rules. If anyone asked who was responsible for security, the answer was that sysprog, "since he's the RACF guy". He didn't have time or resources to do a thorough security program, since he had more than a full time job already as a sysprog.

Then we hired or promoted a RACF administrator, who had no authority to say NO. If anyone asked who was responsible for security, the answer was that RACF admin, since "he's the RACF guy".

Then the auditors came by and wrote up any security weaknesses they could identify, addressing their findings and recommendations to the RACF admin, since "he's the RACF guy".

Some of their findings related to things the RACF admin had no authority to change, such as password length and content, BATCHALLRACF, PROTECTALL, and others. Some of their findings related to things the RACF admin had no knowledge about, such as VTAMAPPL, APPL, storage administration, NODES, job scheduling, and tape management. Sysprogs and storage admins and operators would demand OPERATIONS because they "need it to do their jobs". The auditors would write up the RACF admin because "too many people have the powerful OPERATIONS and SPECIAL privileges."

In short, there was an imbalance between the authority the RACF admin had and the responsibility he or she bore. And there was a knowledge imbalance: It was unfair to expect the RACF admin to have the knowledge of every sysprog.

But if anyone asked who was responsble for security, the answer was the RACF admin, since "he's the RACF guy".

In a few cases, smart auditors recognized these imbalances and made recommendations addressed to the entire organization, regarding IT governance (that is, who is responsible for what). These recommendations included assignment of responsibility and ownership to the right managers for approving the granting of SPECIAL and OPERATIONS, and for deciding whether and how to use various resource classes. They gave the RACF admin the authority to say NO if someone didn't provide written approval from the right manager.

And then IBM added USS, TCP/IP, MQ series, DB2, Policy Agent, ICSF, encryption, and other great new features to z/OS. And for each of these, we know who is responsible for getting them secured. Clearly, it's the RACF admin, since "he's the RACF guy".

Or is it different in your shop?

What Is a Finding?

We asked David Hayes to provide advice for IT staff on what auditors mean when they "have a finding". Here is his answer:

"Get All of the Parts of an Audit Finding

When your auditors inform you that they have *found* something, make sure you get the entire story. Every valid audit finding has four components and should include one or more recommendations for corrective action that specifically address the problem the auditors believe are relevant to what they have identified and their audit objectives.

The first component of a finding is obvious – **the condition**: the auditor's factual description of some aspect of your control environment that does not adequately correspond to the standards you are being audited against.

The second component is called **criteria**, those standards referred to in the preceding sentence. Effective audits are based on auditors doing extensive preliminary research of the relevant and applicable criteria that apply to your organization and are consistent with the purpose of the audit. Keep in mind that relevant criteria can (and should) include technical standards (from respected sources, especially from vendors), your own organization's documented policies and procedures, and regulatory edicts that apply.

The third component is a **factual, supported description** of why the problem exists. This is an important and frequently overlooked part of an audit finding. Unless the cause of a problem is identified, how can effective recommendations for corrective action be made?

The last component of an audit finding is **effect**. Quite literally, the auditors must be able to describe in detail how the problem they have identified has a bearing on your organization's ability to achieve a relevant control objective. The tremendous flexibility of the IBM mainframe computing platforms provides a multitude of techniques available for achieving a level of control consistent with your organization's control objectives. Some of the auditors engaged in audits involving IBM mainframes may not be cognizant of all of the relevant controls you have in place for a specific operational control objective.

Recently, an audit team cited a datacenter for not having effective controls over monitoring because a certain data field in a log file was not populated with the user's ID. They were using one of the STIGs from DISA as their criteria. What these auditors did not know, or take the time to find out, was that other logging (in the same log file) DID include the user ID. These auditors were using a list and when a setting didn't match their list, they were concluding that something was wrong. When asked about the fourth component of their finding, these auditors could not show that anything adverse would occur due to not recording a user ID multiple times in the same monitoring log.

Two lessons to take from this are: find out if the criteria the auditors plan to use is relevant and appropriate and require that any audit finding contains all four components. When these lessons are followed, auditors and organizations will obtain more value from audits." Thanks David.

Statement of good security practices (from IBM, here's a useful starting point)

"IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of your systems to attack others.

Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party."

NYRUG (New York RACF Users Group) Now Extended to Dallas, TX and Raleigh, NC as well as Tampa, FL RUG

May 15, 2019 from 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa and Raleigh and Dallas , a joint meeting by teleconference with all these RUGs.

The meeting after that will be in the Fall of 2019.

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, agenda, copies of handouts and to register, please visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.

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
- Articles from http://www.stuhenderson.com/Articles-Archive.html
- White papers from http://www.stuhenderson.com/XARTSTXT.HTM
- Newsletters from http://www.stuhenderson.com/Newsletters-Archive.html

HG Effective RACF Administration Training and Mainframe Audit 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 RACF administration 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.

HG04 **Effective RACF Administration** (**$2195**)

November 4-7, 2019 in Bethesda, MD

For mainframe audit training, please see: www.stuhenderson.com/XAUDTTXT.HTM.

HG64 **How to Audit z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)

November 18-21, 2019 in Bethesda, MD

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

stu@stuhenderson.com

For Back Issues of this Newsletter, Subscriptionsand 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 iswww.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**

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

To protect voting machines fromhackers,
See the article at
http://www.stuhenderson.com/ProtectVote.pdf