RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 88):

This Issue's Themes:

- Prepare for RACF 2.2
- Secure FTP and USS Sensibly

Free Webinar Hosted by NewEra Stu Henderson will once again present on the z Channel Tuesday and Thursday, November 17 & 19, 2015 - 2 pm EST (11 am PST) **"*How to Go About Setting Mainframe Security Options*"** shows you how to go about deciding how to set security options in RACF, ACF2, or TopSecret.

This presentation won't attempt to tell you how every setting should be set; it will show you how to think about them for yourself in ways that make life easier and security more reliable. For info, or to register for this free session: http://www.newera-info.com/Stu_Henderson.html

(You can also see there handouts from earlier webinars, including "***Top 12 Mainframe Security Exposures and Lessons From A Real Mainframe Break-In***", "***JUST FOR CIOs - Managing Mainframe InfoSec More Effectively***" and "***How to Secure Mainframe TCP/IP***")

Free Webinars by Top Speakers:

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

NEW YORK RUG Meeting Date

Friday, November 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 Spring 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

"*If you aren't challenged, you can't change" — email tagline*

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, people can contact glory.wade@go2vanguard.com.

To subscribe to this newsletter, or for back issues:

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

RACF and z/OS 2.2 New Security Features:

Now that this latest release of RACF is available, you'll want to learn a bit about its new features. The next NYRUG meeting will provide a lot more detail. There doesn't seem to be anything big and complicated here, just small polishing of an already competent product:

- New, advanced encryption for passwords and password phrases, using an algorithm named **KDFAES** (Key Derivation Function with AES) instead of DES. (Note that this is only relevant if someone has read access to a copy of your RACF database.) You will want to implement this, but note that it is a major effort with a few small pitfalls to watch out for. See Bruce Well's presentation at the last NYRUG meeting (handout at http://www.stuhenderson.com/Handouts/NyRug2015TakingTheSwordOutOfPassword.pdf for more details You'll use the command **SETR PASSWORD(ALGORITHM(KDFAES))** to implement this. Note that the default Health Check will notify you if you haven't yet converted to KDFAES.

- **SETR PASSWORD(SPECIALCHARS)** allows the following special characters to be used in passwords and password phrases:

  . (period) < + | & ! * - % _ > ? : =

  (Note: do not implement this until you have tested it with all your programs that have signon screens. Some such programs interpret these characters with special meanings, which can cause problems until you work around them.)

- Two new operands to the **ALTUSER** command are: **PWCLEAN** and **PWCONVERT**. PWCLEAN gets rid of obsolete password history entries in the user profile, for example after reducing the limit with SETR PASSWORD(HISTORY(x)). PWCONVERT can be used to convert passwords in a user profile to KDFAES.

- A new user attribute named **ROAUDIT**. This allows a user to list any RACF profile, issue SETR LIST, and execute DSMON. This is like the AUDITOR attribute except ROAUDIT doesn't give the user the ability to set options which affect logging to SMF. (Note that neither AUDITOR nor ROAUDIT give the user the ability to read any data. Most of the time auditors shouldn't need that ability anyhow.) You might want to give ROAUDIT to any auditor you don't know well enough to give AUDITOR to. Or better yet, use your policy to make someone be the owner of the AUDITOR attribute. "No one is to have the AUDITOR or the ROAUDIT privilege without the written approval of ...". Note that some auditors may have checklists telling them that they need the AUDITOR attribute. Don't hesitate to point them right here while politely suggesting that they get their checklist updated to reflect ROAUDIT.

- New behavior for the **ADDUSER** command: It used to be that if you did not specify the PASSWORD operand on this command, it would default to the value of the DFLTGRP name. As of RACF 2.2, the default password for ADDUSER is to have no password at all.

- A new resource class **FSEXEC** controls Execute access in USS file systems.

- A new profile in the UNIXPRIV classnamed **SUPERUSER.FILESYS.DIRSRCH**

- Various improvements in PKI, RACDCERT, and RRSF.

- **SMF signing** is a way to make sure that SMF records have not been altered. It works like this: for each SMF record, the system calculates a hash total, that is a calculated number which is unique to that message. The system then encrypts the hash total, using two-key (aka asymmetric) encryption and appends the encrypted hash total to the end of an SMF record or group of records. This is similar to the approach used with program signing in the PROGRAM class. If you want to know that the SMF record hasn't been altered, you (or the system) just re-calculates the hash total, and then decrypts the encrypted hash total. If the two hash totals are equal, this is evidence that the SMF record has not been altered. The extra computation may have some effect on CPU usage. There may be regulatory requirements that you implement SMF signing in the future.

So What To Do With RACF 2.2?

First, do nothing for several months after implementing z/OS and RACF 2.2. There's nothing RACF specific that is urgent, and you want to minimize any confusion about causes of any problems.

Then consider giving some or all of your auditors ROAUDIT instead of AUDITOR. The only change this makes is that they can't set options to cause additional logging to SMF. Work this through your formal change control, the way you would any simple RACF changes.

Get more information by attending user group meetings, or seeing the handouts (Please see www.nyrug.stuhenderson.com for latest speakers and the handouts link.)

Then consider how you want to go about passwords, eventually getting to KDFAES, perhaps with special characters. You will want to get to KDFAES, but gradually, as part of a carefully worked plan, addressing all the programs with signon screens and all the programs for RACF administration where you might be typing in passwords. Don't try to figure one password operand at a time. Consider all the password options together in the light of relevant risk, as described in issues 86 and 87 (http://www.stuhenderson.com/RUGNEW86.pdf and http://www.stuhenderson.com/RUGNEW87.pdf .) See password strategy and approach in Bruce Well's presentation at the last NYRUG meeting (handout at http://www.stuhenderson.com/Handouts/NyRug2015TakingTheSwordOutOfPassword.pdf

Address the improvements in **RRSF**, digital certificates and **PKI**, **UNIXPRIV**, and **FSEXEC** as needed, one at a time, as part of your regular change control program. See Mark Nelson's RACF 2.2 Update presentation at the NYRUG or get the handout from http://www.nyrug.stuhenderson.com/handouts.HTM .

APAR Improves SETR Command Behavior for Generics

Joel Tilton has pointed out that IBM has changed the behavior of SETR GENERIC(*) and SETR GENCMD(*) so that they will not enable generics for DIGTCERT & DIGTRING, a good thing. Learn more at:
http://www-01.ibm.com/support/docview.wss?uid=isg1OA48114

Thanks, Joel.

Why POSIX Rigor Matters

POSIX is a standard for UNIX, including UNIX security. There are ways you can relax some of the POSIX standards with USS, ways that may seem convenient at times. These ways can make USS security much more difficult later on. Here's some of the detail, along with description of why you want to avoid loosening the default security.

File security in UNIX, including USS, is based on the directory tree, and the restrictions on which users and groups own a file. For example, unless you have UID(0), you can only change the owner for files you own, and you can only change the owning group to be a group of which you are a member. A little thought will show you why this provides a rigorous framework to maintain tight security.

You can define a UNIXPRIV resource class rule named **CHOWN.UNRESTRICTED** to relax the above restrictions. This may seem convenient, but will later make it difficult to maintain security. This is one of those options which is very difficult to undo, once you turn it on. A good rule of thumb is not to implement any UNIXPRIV rule which relaxes POSIX restrictions on file ownership, unless you have a very good reason, understand the consequences, and are sure of what you are doing.

FTPS vs SFTP or "Do You Need SSH on your Mainframe?"

FTP (File Transfer Protocol) is the protocol with TCP/IP for transferring files between computers. IBM gives us a reliable standard version of FTP for free with z/OS. It can be secured easily with SSL and TLS and a variety of options specified in its configuration file.

Many z/OS shops wanting secure file transfers have been using instead the SSH software with its own FTP program. Apparently there are two ways to implement SSL encryption with FTP. Only one of these works with the free, standard FTP you get with z/OS. The two ways are

- **SFTP**, which is used with SSH, but which doesn't work with FTP on z/OS
- **FTPS**, which works well with the FTP on z/OS, and which works according to the standard described in RFC 2228.

Many FTP clients (the version of the FTP program running for example on your PC and talking to the FTP server program on your mainframe) implement SSL with SFTP, and therefore were not able to talk to the FTP you get with z/OS. However, since FTPS is becoming the standard, most FTP clients are being modified to support it. This means that you may not need SSH, which could simplify your life.

This Issue's Featured Resource Class: VTAMAPPL:

As with most resource classes, the key to understanding the VTAMAPPL resource class is to understand what software calls RACF for it, and when. When your company decides to create a new CICS region, for example, the VTAM and CICS system programmers go out to lunch to decide what to name the new region (or applid, that is, a program with a signon screen). After lunch each sysprog codes the name in a configuration file for the software she manages (VTAM or CICS). When the CICS region starts up, CICS taps VTAM on the shoulder, saying "I'm the applid named ... and I'm here and ready to do work." (The technical term for this is "opening a VTAM ACB", but it's really just a shoulder tap.)

When VTAM gets the shoulder tap, he calls RACF, saying is this user (the userid of the CICS region) allowed to be the applid named ...?") If the class is inactive, or if the class is active and the resource rule allows the access, then VTAM accepts the shoulder tap.

The risk of not using VTAMAPPL is that a rogue TSO programmer could write and execute a program to make the same shoulder tap, spoofing the identity of the CICS region or other applid. The rogue program could then learn users' userids and passwords.

If you decide to use VTAMAPPL, you need the support and participation of your VTAM sysprog. You can collect information without slowing anything down by having just a single resource rule in the VTAMAPPL resource class:

```
SETR GENERIC(VTAMAPPL) AUDIT(VTAMAPPL)
RDEF VTAMAPPL **   UACC(READ) AUDIT(ALL) DATA('BACKSTOP RULE')
SETR CLASSACT(VTAMAPPL) RACLIST(VTAMAPPL)
```

Then collect the SMF data and work with your VTAM sysprog to tighten the rules up slowly and carefully.

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

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet November 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.

Interesting Products:

- **CA Data Content Discovery** helps you identify data exposure risks on z Systems™ by scanning through the mainframe data infrastructure. Data that is scanned includes data that may be highly regulated in multiple vertical sectors or other non-public data sources deemed critical to your business. By discovering where the data is located, classifying the data to determine sensitivity level, and providing comprehensive reporting on the scan results, data can be adequately protected and exposure risks can be mitigated. The data scanning is 100% on the z/OS platform and access permissions are also available so you can easily see who has access to the data identified as sensitive regardless if it is CA ACF2, IBM RACF or CA Top Secret. For more information, please contact Mary Ann Furno at maryann.furno@ca.com

- **NewEra Software's Image Control Environment 14** latest release provides same-day support for z/OS V2R2. Its primary tools have been enhanced as part of this new release. Image FOCUS discovers configuration problems that would result in a loss of z System Integrity or IPL Failure. The Control Editor supports the concept of defense in depth by building a secondary layer of configuration control! ICE/OPER controls, captures and logs the usage of MVS/BCP and ESM Operator Commands. More information is available at www.newera-info.com.

You Can Influence RACF by Voting on This RFE

This Request for Enhancement is to expand the maximum possible length of the RACF (SAF) name for NETACCESS profiles in the SERVAUTH resource class. The RFE number is 78520. You can link to it here:
http://www.ibm.com/developerworks/rfe/execute?use_case=viewRfe&CR_ID=78520

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**)
   December 1-4, 2015 in Bethesda, MD
   March 1-4, 2016 in Clearwater, FL
   December 6-9, 2016 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
   Dec. 7-10, 2015 in Bethesda, MD
   Dec. 12-15, 2016 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
   Nov. 9, 2015 in Bethesda, MD
   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 10-22, 2016 in location TBD

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