RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 90):

This Issue's Themes:

- You need new approaches even if RACF isn't changing much these days. (Perhaps it's approaching perfection?)

Free Webinar "*How to Go About Setting RACF Security Options*"

October 20th at 2pm Eastern Time, with Stu Henderson, sponsored by ASPG. Click here for free registration

NY Metro NASPA (National Association of System Programmers) Meets October 5, 2016 at IBM in New York. For free registration email Mark Nelson ("markan@us.ibm.com") with the subject "2016 October NASPA" Frank DeGilio of IBM will speak on "*Cloud is increasingly focused on providing new capabilities quickly, with security and availability at a low cost. With this goal, the differences that have marked the mainframe as a liability, become a strength to be embraced*."

This Issue's Quiz Question:

"***What Combination of Operands Together Make the SEARCH Command One of the Most Powerful on Earth?***"
(Answer on Page 6)

NEW YORK RUG Meeting Date

October 19, 2016 from 10AM to near 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).** See inside for details. (The meeting after that will be **a Spring date to be determined in 2017**)

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: 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

"One must imagine Sisyphus happy."

– Albert Camus

Vanguard Conference

Vanguard Security & Compliance 2016 is scheduled for November 14-17, 2016 at the Westin Las Vegas Hotel. Here a link with all of the details.

Vanguard Conference Info

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

A Different Approach to Auditing (and What To Do About it)

There is a significant change in the way some auditors conduct IS audits. In the past they would often check settings such as password minimum length as specified in SETR LIST and DSMON against some checklist standard. Any discrepancies would often result in audit findings.

In effect, they just check “security as it is now, a snapshot”.

More recently auditors are being asked to address their analysis in two (or sometimes more) separate steps: Test of Design (**TOD**) and Test of Effectiveness (**TOE**).

In TOD, they evaluate the tools that data center management has provided which are designed to provide effective security. These tools include: policy, standards, procedures, ownership of datasets and resources, RBAC (Role Based Access Control), separation of duties, baseline documents, and risk assessments.

Separation of duties involves understanding who approves access, who puts the access permission into RACF, and who reviews the access permission by comparing rules in RACF to the written approvals.

Baseline documents are documents which specify the standards in a given data center for security settings in configuration files. The baseline is the formal standard against which the actual configuration file settings can be compared. In a RACF audit, the baseline for SETR LIST options for example might be compared to the actual settings.

So under the old audit approach, if your minimum password length didn’t match the auditor’s checklist, you might get an audit finding.

With the newer audit approach, if your minimum password length doesn’t match your baseline document, you might get an audit finding. But also, if you don’t have a baseline document, you might also get an audit finding. (We recognize that audit approaches all along have considered evaluation of management controls. What we are seeing now is greater emphasis on evaluation of the management controls before evaluating how effective they actually are.)

The newer approach asks not just whether current settings are “correct”; it asks first whether your management has provided the resources to define what “correct” is and to stay “correct”. For your management to have provided these resources, someone must have assessed and documented the actual risk you are protecting against, and then developed appropriate baselines, procedures, policy and other controls to reduce the risk to an acceptable level.

Auditors are asked now first to conduct the test of design. If the test of design fails (your management has not provided the resources to understand and manage the risk), then the auditor may be permitted to skip the work required to conduct the Test Of Effectiveness (how well does your design actually reduce the risk). Why bother with the TOE, if the TOD isn’t satisfactory? (“No TOD? No TOE!” as some auditors phrase it.)

For Federal agencies, some of these basic management controls are required. But since the AICPA has recommended the TOD/TOE approach, auditors are starting to follow it in the commercial world. And to implement RACF without your management providing and supporting these basic management controls might be a waste of time.

This is similar to the adage “Give a hungry man a fish and he’ll be hungry the next day. Teach him how to fish...”. Auditors are looking for evidence that you have the tools and information and knowledge to make your operation safe, not just whether you might happen to be safe today.

So how to prepare for such audits? You can’t manage security if you don’t know what risk you are trying to protect against. You can’t know what risks to protect against if you don’t know what you have (hardware, software, applications, data, networks).

So to start, auditors might ask for (and you might want to have at hand), an inventory of your hardware, etc. You might want a formal risk assessment, describing what could go wrong from a security point of view. And you might want to have baseline documents, stating for example, how the SETROPTS options are supposed to be set in your shop and why. Policy and procedures for security administration will be helpful too.

Making sure that your data center has these controls can help your career. But the controls will be most helpful if they are developed and adopted by the entire organization, not some documents one individual threw together in a corner.

What’s the Impossible Security Problem and How to Solve It

The impossible security problem is that some user somewhere sometime will be careless with his (or her) password. You can make passwords be infinitely long, requiring upper and lower case, emoticons, and Chinese characters. This still won’t protect against the user who writes the password on the desk blotter or falls for phishing email scams. There is nothing you can do in RACF alone to fix this. (As a wise man once said, “There’s no PTF for Careless.”)

So how to solve the unsolvable problem? **MFA** (Multi-Factor Authentication) often reduced to **TFA** (Two Factor Authentication). This is the idea that to prove who you are, you need two different types of proof. Usually we require two types of proof, each from a different one of these three categories:

- Something you know (password),
- Something you hold in your hand (key, credit card, security token), and
- Something you are (biometrics, still widely not ready for prime time).

Regulations for Federal agencies are now requiring at least TFA. And mainframes and RACF now support TFA, most commonly with a combination of password and hand-held token such as the RSA tokens. These hand-held tokens generate a unique random number each minute, a number which is unique to your userid and that minute. So you type that random number in with your password when you log on. RACF can check both your password and the number you type in to prove that it’s really you. (Don’t forget to make sure all your programs with sign-on screens support this.)

There are two basic types of hand-held token: **hard** and **soft**. Hard tokens are ones you can hold in your hand or attach to your keychain. Soft tokens are programs that run on your pc and generate random numbers just like hard tokens.

You can see the pros and cons: with soft tokens, you don't have to worry about arriving at work and discovering that you left your token at home on your dressing table. But if you use a soft token on your laptop, and someone steals your laptop, then they've stolen your soft token as well. So you might want to use soft tokens on desktop pc's that are kept in locked rooms. You might want to use hard tokens with laptops you travel with. (And please don't leave your hard token in your laptop bag!)

Smart organizations are starting to implement TFA on their mainframes. The very smart organizations are implementing TFA on both their mainframes and their Windows and UNIX computers, ideally using the same sort of hand-held token on all the computers. (That sounds similar to other issues we've encountered in the past.)

One Key, Many Doors:

Okay, you're thinking, so maybe MFA could be useful in proving who I am to RACF, even if someone has stolen my password. What else could I use this for? Well, if to RACF, why not to Windows? Wouldn't it be great if one hand-held token, along with my password, would let me log onto any of my computers? In fact, it seems sort of half-thought out to use MFA to secure your mainframe access without giving the same protection with the same tools to your Windows computer.

(Some people advocate making the handheld tokens into jewelry, such as rings, tie tacks, belt buckles.)

But don't you have a separate card-key to get into the computer room, or the wire transfer room, or your building or your office? Why not integrate this all into one hand-held token that proves who your are to every computer, and to every locked door you want to open?

How Many Times in Your Life Do You Fill Out Your Name and Address?

While we are dreaming, wouldn't it be nice if you could put your name and address, and maybe email address (but not any of your passwords) into your hand-held token? And every time someone asks you for your contact info, you just wave your token in the air (or press it to the other person's smart phone), and save yourself all that tiresome effort.

I pay for my Starbucks with my Iphone. Why not put every type of "prove who I am" into a single device?

This Issue's Featured Resource Class: UNIXPRIV

The **UNIXPRIV** resource class is used to grant users certain privileges in **USS** (UNIX System Services, the UNIX that comes as part of z/OS).

First a little background: USS does file access control like any other UNIX. Users are identified by a number called a **UID**. And groups are identified by a different number called a **GID**. And every file has something similar to a dataset rule in RACF, called a File Security Packet or **FSP**. (This is the familiar READ/WRITE/EXECUTE sequence.)

When a user tries to read or write a file, UNIX compares the UID and GIDs of the user to the FSP of the file to determine whether to allow or deny the request.

USS is different in this one respect: USS asks RACF to make the comparison of the UID and GIDs to the FSP, instead of USS making the comparison himself. (There is a way to disable this action, but you don't want to do it.)

This has several advantages: security administration is centralized in RACF; so is security logging. And RACF can make addtional checks.

Before RACF compares the UID and GIDs to the FSP, RACF can use rules in the UNIXPRIV resource class to ask "Does this user have special UNIX privileges that override the FSP?"

For example, you might have a UNIXPRIV rule named **SUPERUSER.FILESYS**. **READ** access to this rule lets you read any USS file and search any USS directory. **UPDATE** access let your write to any file, but not to any directory. **CONTROL** access lets you write to any directory as well. There are several other UNIXPRIV rules described in the IBM manuals.

You can see that it makes sense to get out in front of the UNIXPRIV resource class, and get clear definition of who owns it, who approves rules, how they decide what the rules should be.

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

Interesting Products:

While we generally do not endorse or denigrate vendor products, we think these are some you might want to explore and evaluate:

- **Two Products from Fedtke.com: SF-Sherlock** provides real-time monitoring technology for security, compliance and quality on your z platform by integrating monitoring, recording, notification, reaction, reporting and simulation (e.g. IPL) into an overall automation solution. It constantly monitors and examines the security system (Security Server or RACF as well as CA-TSS and CA-ACF2), specific processes and subsystems (DB2, LDAP, etc.) and the z/OS operating system. It records relevant changes in an audit-secure manner and provide real-time notification about events such as errors, attacks, manipulations, etc., e by e-mail, SMS or similar. SF-Sherlock provides constant and complete monitoring, especially at deeper technical levels with the new z/OS functions (USS, Sysplex, etc.) and the new areas of application as web server, data server. A second product: **sf-dumpanonym** eliminates all confidential data from your dump files For more info contact: stfedtke@fedtke.com or see http://www.fedtke.com

- The **Beta Systems RACF Security Suite** supports user-friendly administration and security monitoring. A single point-of-control for the administration and auditing of multi-CPU environments with: Automatic generation of RACF commands, Simultaneous update of multiple RACF profiles, Cross-checks for identifying invalid definitions, Administration of multiple CPUs, Online RACF data analysis from different RACF databases , Policy definition for regular audit tasks, Real time monitoring of security events. The Web Help Desk helps large organizations manage high volume RACF administration requirements. Beta Enterprise Compliance Auditor is a comprehensive monitoring tool. For more info, contact: Christopher Luzins, phone: +1-215-680-9104, or christopher.luzins@betasystems.com or http://www.betasystems.com

- **Wintrac** is a technology training company that has an extensive including COBOL, CICS, DB2, Easytrieve, FileAid, ISPF, JCL, VSAM, IMS, JES2, REXX, SysPlex, SMP/E, Xpeditor and z/OS. These courses can be customized and delivered onsite or online. Detailed course outlines at http://www.wintrac.com/courses/coursesmain.asp Details at www.wintrac.com

Answer to This Issue's Quiz Question:

"***What Combination of Operands Together Make the SEARCH Command One of the Most Powerful on Earth?***"

Use the SEARCH command in RACF with the CLIST operand to build a CLIST of RACF commands. In the CLIST, use the FROM, FCLASS, and FGENERIC operands to copy rules from one class to another. For example, suppose you have a bunch of RACF rules in the ABC class, and you want to make identical rules in the XYZ class.

SEARCH NOMASK CLASS(ABC) CLIST('EXEC MYCLIST ')

then define MYCLIST to issue **RDEF XYZ &1 FROM(&1) FCLASS(ABC) FGENERIC**
What other uses can you imagine for this technique?

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet
October 19, 2016 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**)
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**)
September 19-22, 2016 in Chicago
Feb. 28-March 3, 2017 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. 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