RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 82):

This Issue's Themes:

- Things we can learn from auditors
- Who's Responsible for What?

Chicago RUG Meets February 20

Contact Patricia Diya for details and to get on her mail list:

EML patricia.diya@acxiom.com
TEL 630.944.5142

Barry Schrager to Discuss Security Issues

Before becoming President of Xbridge Systems, Barry did some interesting things like invent ACF2. Xbridge will be sponsoring a free breakfast in May in NYC where you can hear him discuss challenges in the mainframe environment. To learn more, visit xbridgesystems.com or call 845-837-1087.

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, March 12, 2013 from 10AM to around 4PM.

Because of Hurricane Sandy, our meeting site has moved to IBM at 590 Madison Avenue. This has complicated video-conferencing with Tampa. Please check the website a few days before to learn how the video-conferencing is going.

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 2013**)

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

"*Tell me and I'll forget; show me and I may remember; involve me and I'll understand.*" ***- Chinese Proverb via RACF-L***

Vanguard Conference June 24-27, 2013

This great conference will be held June 24-27, 2013 in Las Vegas, NV. Learn more at:

www.go2vanguard.com/conference.php

Newest Release of RACF Announced

IBM has announced the latest release of z/OS. It's number 2.1 and should be available in September. And with it comes, you guessed it: RACF for z/OS 2.1. We now expect new releases of z/OS (and of RACF) every two years instead of twice a year. When your product approaches perfection, you don't have to update it so often.

RACF, PCI, and DES

A friend emailed a problem he was having with a PCI compliance auditor.

(PCI is of course the Payment Card Industry standard. The credit card companies got tired of companies not providing good security to protect credit card numbers. So after years of asking companies to comply with their standards, they decided to charge any company that failed to follow their security standards a few cents per transaction. This adds up to big money. And introduces a whole new kind of audit: a PCI audit to determine if you are in compliance with their standards.)

Unlike some types of audit, PCI audits can cost your company serious money if you fail them. This auditor was claiming a PCI violation because the company uses RACF for security, and (the auditor's logic went) RACFuses DES encryption, and DES is "easily crackable". The implication was that the company needed to switch to some other security product to pass the audit. (Both ACF2 and TopSecret have recently added an option to use AES encryption, a standard that is newer than, and considered stronger than DES. RACF uses only DES.)

The flaw in the auditor's argument was of course that RACF uses DES to encrypt passwords, not to encrypt credit card information. RACF does not encrypt credit card information at all. That is not RACF's job; it is the job of some other hardware or software.

Plus, you can't crack anything in the RACF database unless you can read the RACF database. And none of us lets anyone read the RACF database since it would then be possible to run a password cracker program and learn everyone's userid and password. And even if RACF did use AES, a cracker program could still crack the passwords anyhow (even if it might take longer.)

So what lessons can we take from this?

- For RACF's purposes, DES is more than good enough
- When auditors make wild leaps of logic, it is worth helping them to have a sounder understanding
- It is easy when an auditor makes a strong claim to forget to question the logic behind it. Back it up; slow it down; let's walk slowly and carefully down that path again together. Let me hold your hand firmly so you don't trip.
- RACF would be out of business if it would cause PCI audit failures. It's not.
- Much more important than the encryption algorithm is restricting read access to the RACF database and its backups.

Quick, Easy Check to Improve CICS Security

An auditor once tried to execute a powerful CICS transaction without signing onto CICS first. (That is, he had a bind linking his terminal to the CICS region, but had not entered a userid and password to prove who he was.) He was surprised to see the transaction starting to execute, and wondered how this could be.

Later research provided the explanation: the default userid for the CICS region had been permitted to the powerful transaction. When the auditor entered the transaction name, CICS had no ACEE (user definition) for him since he hadn't signed on yet. In this case, CICS always calls RACF with the ACEE of the default user, and so the transaction was permitted.

Since then, several audits at other locations have identified permissions for the default userid in CICS which should not have happened. How can you protect yourself against this? With a little-used option of the SEARCH command in RACF.

With SEARCH you can specify both a classname and a userid (with the USER(xx) parameter). So if the default userid for a CICS region is GEORGE, then you would issue

SEARCH CLASS(TCICSTRN) USER(GEORGE) and

SEARCH CLASS(GCICSTRN) USER(GEORGE)

to learn all the rules in those classes to which GEORGE is permitted. Then gently remove any improper permissions.

Some smart auditors are starting to make this part of their audit program. But you can beat them to the punch.

New Blog for IS Auditors (But You Can Look and Comment Too)

It's at www.stuhenderson.com/isauditblog . Let us know what you think.

Interesting Products

Eb Klemens of EKC always has interesting things to say. The most recent is "***Rankings help discern patterns***." He has several new products which illustrate this, as well a new page on his website with hints and tips for RACF administrators. You can see it at www.ekcinc.com .

What Do They Mean By "IT Governance" and How Can It Help Me?

Auditors sometimes talk about IT governance as if it's important. And it is. It is the concept that your organization should clarify in writing who is responsible for what. How does this affect the RACF administrator? It protects him from what Russ Hardgrove calls "RACF – Guilty Until Proved Innocent".

If there's a security problem of any kind and the IT governance isn't clear, then it's likely that you will receive some finger-pointing, since "You're in charge of security, aren't you?". It's unfair to expect the RACF administrator to take care of things he or she doesn't have the authority or knowledge to address. For example,

- You may not have turned on ERASE-ON-SCRATCH because the system programmer told you not to. Or if you did turn it on, you didn't know which datasets to apply it to. Likely the owner of the application, the Legal Department, or the Compliance Department has that knowledge. If your policy doesn't state that those with the knowledge should tell you where to apply EOS, and then you should carry out what they decide, then you are caught in a lose-lose situation. You auditors might help make this better by making a practical recommendation to improve IT governance.

- Your auditors have recommended that you "review the violations report each day". Your boss buys you bottles of Excedrin in sympathy, but doesn't volunteer to pay for your new eyeglasses. Your review makes no difference because you don't have the authority to tell anyone except the RACF intern to change his behavior. If the auditors wanted to improve IT governance, they might change their recommendation to be that supervisors should be responsible for dealing with violations by their direct reports. And that RACF administration should track trends and patterns in RACF violations to identify where improvement is possible.

- If you haven't activated the VTAMAPPL or SERVAUTH resource classes, it's probably because you don't know what they are for, and your VTAM system programmer never told you to turn them on. You don't have the knowledge or authority to turn them on. Good IT governance would clearly assign authority to the right staff to decide whether and how to use each resource class.

- How do you decide whether to give someone SPECIAL or OPERATIONS? Do you make a judgement call based on whether you think it's "appropriate to their job"? (There's a mushy standard for you.) Good IT governance might assign someone else the authority to decide who gets RACF privileges, and assign you the responsibility to carry out their decisions.

In all of these situations, clarifying what you are responsible for, and what not, will improve your ability to do your job well. It will also improve the quality of your organization's security. Your auditors can help to make this happen.

Sorting Out an New Application

It happens sometimes that system programmers install a new software product or program without telling RACF administration. Later someone tells the administrator to “secure it” without any documentation or useful information. Here are some steps to follow to investigate it:

1. The program will have JCL stored in a proclib. Browse the JCL to find out what the name of the program, the datasets it uses, and its userid. Verify that the userid doesn’t have OPERATIONS, UID(0), or SPECIAL.

2. If it’s a started task, check the DSMON report to see what the userid is. If the DSMON report says that the started task is either TRUSTED or PRIVILEGED, then every time it calls RACF to ask permission, RACF immediately says “YES”.

3. If the program is online, it will be defined to VTAM as an applid. (An applid or application identifier is a program with a signon screen.) If it is, you may be able to control who can use it by means of the APPL resource class. (You might also use the name of the applid as the name of a rule in the VTAMAPPL resource class, but only under the direction of the VTAM system programmer.)

4. If the program is online, it may or may not call RACF to verify the userid and password. If it doesn’t, then it probably uses a hard-coded list of userids and passwords. This means that RACF can’t control access to it. It also means that the APPL and TERMINAL resource classes have no effect on it. You might think of this as a path into your system that is not controlled by RACF. It means that if someone who uses the program is fired for dishonesty and you revoke his RACF userid, then he still has access to the system. You, the RACF administrator have no way to cut him off at this point.

5. If the program uses TCP/IP, you might be able to control its use with the SERVAUTH resource class.

6. If you know the name of the library where the program lives, you might be able to control its use with the PROGRAM resource class.

7. If the program is defined in the Program Properties Table with a YES under BYPASS PASSWORD PROTECTION (see it in your DSMON report), then RACF does not get control when the program opens a dataset.

8. If the program was installed as a privileged program (that is, with the privileges of MVS, which allow it to bypass RACF altogether), someone should want to know that the program can be trusted. This means that the program doesn’t introduce security exposures to your system. There are several way a program can receive these privileges, including APF authorization and User Supervisor Calls. Unless you are a system programmer, there is little you can do to secure this.

9. All of this should make you wonder about your organization’s policies and procedures and IT governance. This might be a topic to discuss with your manager.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
March 12, 2013 from about 10AM to 4PM:

Our next meeting is at IBM, 590 Madison Avenue in Manhattan. (Hurricane Sandy knocked out our previous site at DTCC.) This is usually a joint meeting by teleconference with the Tampa FL RUG. But we have not yet been able to sort out the video-conferencing. Members of the Tampa Bay RUG will need to check our website a few days before the meeting to see the latest developments.

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 both meetings 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**)
Feb. 26-Mar. 1, 2013 in Clearwater, FL
Dec. 2-5, 2013 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
May 20-23, 2013 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
April 11, 2013 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, and DB2** (**$2100**)
March 25-28, 2013 in Chicago, IL
May 7-10 , 2013 in Raleigh, NC

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)
April 8-10, 2013 in Bethesda, MD

C) HG76 **How to Audit TCP/IP Security ($575)**
May 29, 2013 in Bethesda, MD

D) HG76 **How to Audit UNIX and Windows Security ($2200)**
September 9-12, 2013 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, Free Newsletter subscription, Seminar Catalogs:
Stu Henderson - (301) 229-7187
5702 Newington Rd, Bethesda, MD 20816

For Back Issues of this Newsletter 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 learn more about the Mainframe Audit News (MA News), check Stu's website at www.stuhenderson.com/XMANETXT.HTM.

To Get a Free Subscription to the RACF User News Phone Stu at (301) 229-7187 with your request, leaving your name, email address or postal address (sorry, only US postal addresses; others will need to read issues online), and phone. For back issues and articles on topics like the **SERVAUTH** resource class, check his website:
www.stuhenderson.com

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 software and tape management software