RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 76):

This Issue's Themes:

- Missing the Point
- If It's No One's Job, It Won't Get Done

CA's May Mainframe Madness:

Computer Associates is running a month long, free, Internet-based, opportunity to learn more about IS security and audit. Learn more at: www.ca.com/us/content/campaign.aspx?cid=200004

Want to Reduce the Number of Users with OPERATIONS?

Your storage administrators will need some other way to do their job before you can take OPERATIONS away from them. You can do this with the **DASDVOL** resource class, and with **FACILITY** class rules whose names start **STGADMIN.**. Here's what the IBM manual for storage administrators says on the subject: "*The storage administrator must work with the security administrator to give authorization to user and storage administrator commands*."

The details of the rules in RACF to control storage administrator commands are in this IBM manual:***"DFSMShsm Implementation and Customization Guide"*** Order No.:SC35-0418-10

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, May 11, 2010 from 10AM to around 4PM. PLEASE NOTE THIS IS A SPECIAL MEETING WITH DIFFERENT TIMES AND REGISTRATION REQUIRED. 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,

---

NY Metro NaSPA Chapter (system programmers professional association) meets Oct. 19 at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 5:00 PM. You are warmly invited. Please RSVP to Mark Nelson at markan@us.ibm.com

The meeting is open to non-NaSPA members and is free! Please pass this invitation on to your colleagues!

Vanguard Conference April 19-22, 2010

This great conference will be held April 19-22, 2010 in Las Vegas, NV. Learn more at:

www.go2vanguard.com/conference.php

Today's Quotation

"*There are 10 types of people: those who count in binary and those who don't*"

Which Started Tasks Should Be Marked Trusted in the RACF STARTED Class?

IBM tells us (in the manual "***z/OS MVS Initialization and Tuning Reference***") that we should not give a started task (procedure) the TRUSTED attribute unless you have product documentation telling you to do so, or it is in this IBM-supplied list:

CATALOG, DUMPSRV, IEEVMPCR, IOSAS, IXGLOGR, JES2 or JES3, JESXCF, LLA, NFS, RACF, RMF, RMFGAT, SMF, TCPIP, VLF, VTAM , XCFAS and optionally:

APSWPROA, APSWPROB, APSWPROC, APSWPROM, or APSWPROT; DFHSM, DFS, GPMSERVE, OMVSKERN, SMSVSAM

Who Decides, Who Has the Knowledge, Who Gets Blamed?

What are the answers to the above questions in your shop for these situations?

1. Some sensitive dataset (say the customer master file) is sent over the network without being encrypted. Some rude person without authorization copies it from the network and sells it to your competitor.

2. Some employee copies a file containing customer credit card numbers onto his laptop "to do financial analysis". His laptop is stolen and some rude person uses the credit card information to buy things. The whole story hits the newspapers.

3. An APF-authorized library is created with a dsname that puts it under the protection of a RACF dataset rule which allows anyone to update it. A contractor writes a program containing a MODESET, moves the program into the library, and uses it to update the Accounts Payable file of checks to be written.

4. On the request of the Sales Department, a new order entry system is developed which processes orders over the Internet. The new system uses DB2 and CICS on the mainframe. The developer uses SSL to encrypt all the transactions. However a hacker uses SQL injection to cause the system to garble all the orders, changing item numbers, quantities, and prices to random values.

5. FTP on the mainframe is set up to allow production control staff working from home to submit batch jobs to execute on the mainframe. One programmer, actually a contractor working from another country, uses FTP to browse the check register printout every time Payroll runs.

6. Many similar situations involving incomplete security, including: spoofing of VTAM applids, copying of sensitive residual data from disk, hard-coded lists of userids and passwords, APPN connections with Enterprise Extender, and other possibilities.

In each case, the auditors explain that they have followed their procedures, and completely documented their work.

In many of these situations, the person responsible for mainframe security (isn't that the RACF administrator?) is likely to be blamed. He or she may not have known about the decisions being made that led up to the incident.

He or she may not have the knowledge (technical knowledge, regulatory knowledge, business knowledge, risk knowledge) to evaluate the situation. It may be that no one had been made responsible for addressing a given issue, but if it involves security, we assume that it was the RACF administrator's job. What can you do to protect yourself before this sort of stuff happens in your shop?

A. Make your management aware of the issues and get their help in defining what your are responsible for and what you aren't. Get their further help in setting up procedures to be followed to include security staff in new application design and review.

B. Ask your auditors to address their audit to the question "What needs to be done to make security on this computer system as good as it needs to be?" Ask your management to ask them too.

C. Identify information you need which is not available to you. Get help in making it come to you, or in making it someone else's responsibility to deal with it. This includes new applications, new network connections, new technologies that affect RACF and mainframe security.

Some installations now require a formal risk assessment to be performed for each application. The people responsible for this include: the business unit heads, and the heads of these departments: Legal, Regulatory Compliance, Risk Management and Insurance. The risk assessment should document what laws and regulations (including records retention regulations) apply to which datasets and fields in those datasets. The risk assessment can include data classification by sensitivity and by criticality (for disaster recovery planning).

The risk assessment provides specific direction to RACF administrators and other IT staff regarding which data is to be encrypted and which datasets are to be protected with ERASE-ON-SCRATCH. If there is any question about performance problems with ERASE-ON-SCRATCH, the system programmers are consulted. The RACF administrator then carries out whatever the risk assessment (including the system programmers' input) directs.

Some Follow-On Questions:

If you have TCP/IP on your mainframe, and you use it to support daemons like FTP, each daemon can have a control file where security options are set. We'll use the FTP daemon as an example.

It's control file can specify:

- What encryption (like SSL) to use when sending / receiving data over the network
- How users are identified (for example, as anonymous without requiring a password)
- Whether users on the Internet can submit batch jobs, browse DB2 tables, and review printouts on the print queue

(Cont'd)

(Cont'd)

Do you think there should be formal change control and quality assurance over the FTP control file? Do you have this control in your installation? (It may likely be a USS file.) How good is your USS file security? Does your production quality control process or your system software quality assurance / change control process extend to the control files for daemons that specify which keyrings and digital certificates are used?

Does your TCP/IP administrator understand BATCHALLRACF? What the print queue is? What a batch job is?

What Is a Site Certificate?:

You know that there are three types of digital certificate you can have in the RACF database:

- **CA or Certificate Authority certificate** used to certify or authenticate other digital certificates. CA certificates are always owned by the userid **irrcerta**.
- **User certificate** used to represent a user
- **Site certificate** Site certificates are always owned by the userid **irrsitec**. They are unique to RACF. A site certificate contains the private key as well as the public key of the matched pair. You use them when you want to share a pair of keys (one public, one private) with a single digital certificate among several programs (servers like FTP, httpd, etc.) in a single data center (or site).

A **site certificate** can be shared among userids and makes the private key of the pair available to more than one user. Suppose for example that you have several daemons (like FTP or httpd) on different CPUs (or even in different data centers). Each CPU has its own RACF data base. Each daemon has its own userid defined in its RACF database. You can share a single site certificate (with a single pair of keys) among all these userids.

You import the site certificate into every RACF database involved. You'll have to create one keyring for it in each RACF database (since keyrings only work within the scope of a single RACF database).

You would consider using a site certificate any time you want to have several userids share a single private key. (For example, suppose you want to support encryption between two daemons, but you don't need to prove their identities to each other.) You would use a site certificate because you can't do this sharing of a single private key with vendor supplied CA certificates. Vendor supplied CA certificates (such as those from Verisign) never contain the private key.

You can't do this with a user certificate for this reason: Unlike other platforms, RACF on the mainframe makes the private key for a user certificate available only to the userid associated with the certificate. This is more secure than for example a UNIX computer, where any user who can access the key database can access every private key in it. This is just one way that RACF provides more secure digital certificates than other platforms do.

Data Protection Self-Assessment:

Here's how to do a systematic self-assessment of how well you protect your data. It will prepare you well for any upcoming RACF audits.

Step 1 Basic Setup:

You will want to know the following, and be able to document why they are the way they are: PROTECTALL, which userids have OPERATIONS (beyond the Firecall ids), which started tasks are marked TRUSTED or PRIVILEGED. (Please see IBM-supplied list of such started tasks earlier in this issue.)

_____You will also want to be able to document who has what permission to what datasets. Imagine that you are an auditor who has listed some of your installation's RACF dataset rules. You need to comment on whether the protection is adequate. Since you're an auditor from out of town, your own opinion is meaningless. So you will either use whatever checklist or methodology you have, or rely on what the RACF administrator has. If he offers you an official list of the owners of the applications, along with access requests signed by the owners, and if the requests match what's in the RACF dataset rules, then the auditor can ignore his checklist. In effect, the RACF administrator is helping the auditor to skip his checklist by offering him a better standard to compare against.

Step 2 Tape Protection:

Tape datasets can be protected by dsname and by volser (tape cartridge). Dataset protection can be turned on for tape with SETR TAPE, but you may want to address it in tape management software or in the parmlib member DEVSUPxx instead. You'll want to be sure that you are addressing BLP (Bypass Label Processing), the 17 character dsname problem, and residual data. (Please see Issue 74 for more details.)

Step 3 Disk Protection (Including USS Files):

For MVS files, have written approvals and/or annual re-certification telling you what the permissions should be for each dataset. Use ERASE-ON-SCRATCH, but most likely only on selected datasets, as other people direct you. Give permission to groups, not to userids. Consider using RACF groups to represent roles, as in Role Based Access Control (RBAC).

A good rule of thumb is that if you have more than three or four dataset rules per production application, you have probably let things get more complicated than they need to be.

Another rule of thumb is that if you have more than four or five entries in the permit list of a dataset or resource rule, or if there are a lot of userids in the permit list, then you probably have let things get more complicated than they need to be.

For USS files, consider using ACLs (Access Control Lists). But before you do that, simplify things by using this feature of UNIX: No one can access a UNIX (USS) file unless he has EXECUTE permission to every directory and sub-directory in its path. So for example to separate Production from Test, have a directory named **/Prod**.

Create a RACF group, perhaps named **GRPPROD**, with a GID in its OMVS segment. Make that GID be the owning GID of the directory **/Prod**. Set the permission bits for that directory to give only the owning UID and owning GID of the directory EXECUTE permission to it.

The result of all this is that if you connect a RACF user to the RACF group **GRPPROD**, then you have given him access to that branch of the USS file directory tree. You can then make subdirectories, named for example **/Prod/Payroll**, **/Prod/Sales**, etc. This would be comparable to naming MVS datasets **PROD.PAYROLL**.., **PROD.SALES.**.., and so on.

Step 4 Printouts (SPOOL) Protection:

_____Be sure to use the JESSPOOL resource class to protect printouts on the print queue.

Step 5 Encryption:

_____You can't control encryption with just RACF. Make sure it is clear who in your organization is responsible for providing encryption where needed.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
May 11, 2010 from about 10AM to 4PM:

Our next meeting is at DTCC in downtown Manhattan. This is a joint meeting by teleconference with the Tampa FL RUG. Attendees **must present a government issued photo ID** to enter the 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 to Hayim Sokolsky (hsokolsky@dtcc.com) with "NYRUG" or "Tampa RUG" in the subject line and your name, company, phone, and email.
You must register for the NYC meeting in advance. (Click here)

Please note that speakers no longer provide copies of handouts. You can print your own copies from this link: www.stuhenderson.com/XMAINTXT.HTM#handouts . Our exact agenda is not certain at press time, so you might want to check this link for exact details as they become final: www.stuhenderson.com/XMAINTXT.HTM#nyrugref .

The nearest subway stops are the Wall St. Station (2 and 3 lines); Bowling Green Station (4 and 5 lines); and Whitehall St Station (R and W Lines). The Staten Island Ferry is close by.

The Tampa Meeting will be at 18301 Bermuda Green Drive in Tampa. (You take I 75 North to exit 270 (the Bruce B Downs Blvd (CR 581)). Bear right at the at the end of the ramp, then at the 2nd traffic light, turn left onto Highwoods Preserve Parkway for .6 miles and turn left onto Bermuda Green Drive.
You must register for the Tampa meeting in advance. (Click here if reading this online)

For complete directions, please go to: www.stuhenderson.com/NYCRUG1.pdf Or to: www.stuhenderson.com/TampaRUG1.pdf .
(cont'd)

(cont'd)

Speakers (subject to change) may include:

- **Anne Lescher** of IBM on "*IBM Security Solutions Update*"
- **Hayim Sokolsky** of DTCC on "*RACF and ICSF, Delegated too!*"
- **Mark Nelson** of IBM on "*Staying Current as the World Rushes* by"
- **Mike Onghena** of IBM on "*IRRXUTIL: Getting RACF profile data directly into REXX programs without parsing*"
- **David Hayes** of GAO on "*Lessons Learned: Tales from Recent Audits*"
- **Wai Choi** of IBM on "'*Digital Certificates TidBits'*
- **Jeff Benson** of Guardian Life Insurance on "*Little Known Features of Vanguard Administrator*"

HG RACF Training Schedule:

The Henderson Group offers its RACF and computer security/audit seminars around the country and on-site too. See the details below or call (301) 229-7187 for a free seminar catalog. For more info or to see what students say about these classes, please go to **www.stuhenderson.com**. (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**)
Dec. 6-9, 2010 in Bethesda, MD
Mar. 1-4, 2011 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($2050)**
May 23-26, 2011 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
April 11, 2011 in Bethesda, MD

HG Mainframe Audit Training Schedule:

The Henderson Group now offers its series of "How to Audit.." seminars for IT 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** (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.)

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$1980**)
May 4-7, 2010 in Raleigh, NC
Nov. 16-19, 2010 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)
April 6-8, 2011 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.

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:**www.stuhenderson.com** .

To Get a Free Subscription to the RACF User News Phone Stu at (301) 229-7187 with your request, leaving your name, 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 or three 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.

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 ..
- Steve Neelands's RACF page is **www.geocities.com/steveneeland/**
- 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
- IBM Redbooks site: www.ibm.com/redbooks
- IBM z/OS Manuals: www.ibm.com/servers/eserver/zseries/zos/bkserv/
- (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 in the following article from the zJournal:

http://www.zjournal.com/index.cfm?section=article&aid=762