RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 81):

This Issue's Themes:

- Doing a Complete Job of Implementing RACF
- Taking Advantage of Standards
- Big Changes From IBM to Simplify Our Lives

New Format for NYRUG and Tampa Bay RUG

Our meetings will now include a Five Minute Madness, a tutorial, discussion of requests to pass onto IBM for RACF improvements, and other innovations. Please see details inside this newsletter.

New Redbook Shows How to Connect z/OS to Smartphones

Just in time for Halloween, IBM shows us how to let users with Smartphones use them to access the mainframe. See the redbook at: http://www.redbooks.ibm.com/abstracts/sg247836.html

New Website for the NYRUG: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG at

www.nyrug.stuhenderson.com

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, October 23, 2012 from 10AM to around 4PM.

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 Spring date to be determined in 2013**)

Today's Quotation

"***When you hear hoofbeats, think horses, not zebras."***

Chicagoland RACF User Group Meets October 4, 2012

For more info, please contact Patricia Diya at patricia.diya@acxiom.com

Free Training in WebSphere and RACF

From Mike Kearney of IBM (who is a great instructor and who knows Websphere) in the Tampa area, first quarter of 2013. You pay your own travel expenses, but tuition is free if you register in time. Please email Stu at stu@stuhenderson.com to express interest. This will get you a place at the head of the line as details shape up. The class is two and one half days.

IBM Slows Roll-Out of New Releases

Soon we'll expect new releases of z/OS (and of RACF) every two years instead of twice a year. IBM' has issued a "*Statement of Direction z/OS*" dated April 11, 2012 which details some major changes in the z/OS "release cadence". This will all start with z/OS Version 2, that is, z/OS 2.1 which might be expected in the last half of 2013.

Along with these system software changes come new hardware requirements for CPUs and for storage control units.

Ways a Dataset Can Avoid RACF Protection

When evaluating dataset protection, you will want to be aware of all the ways a dataset can be NOT protected. Here's a list, in no particular order.

- Datasets with access allowed due to entries in the Global Access Table
- Programs marked NOPASS in the Program Properties Table
- Users with the OPERATIONS attribute
- Users with the SPECIAL attribute with PROTECTALL active and no matching rule
- Started task marked TRUSTED or PRIVILEGED in the STARTED PROCEDURES TABLE (see your DSMON report)
- Dataset rules with WARNING
- Residual data on tape and disk
- Databases mirrored over a sysplex with different RACF databases
- Data on shared DASD (shared disk between CPUs or LPARs) with different RACF databases
- Users who Bypass Label Processiing for tape datasets
- Users who bypass tape security by abusing 17 character dsname in label.

Blocking the Ports for TCP/IP Security

Remember when we were trying to implement PROTECTALL, and everyone got mad at RACF because everyone wanted the freedom to name his own datasets? And how much easier life was, once everyone just followed the naming standards that PROTECTALL forced them to follow?

Ports in TCP/IP may present a similar opportunity. A port is a path into your system through TCP/IP. It usually corresponds to an application, for example email is often used with port 25. However, any port which is not "blocked" or reserved is available for any program to open, after which the program can do reads and writes over the network. Your installation can control who is allowed to open a port by settings in the TCP/IP control file, and also with the RACF resource class SERVAUTH. You might want to have lunch with your TCP/IP admin to discuss this all..

New STIG

NIST has a new STIG (Security Technical Information Guide) for RACF. You can download the most recent STIGs for RACF, ACF2, and TopSecret from: http://iase.disa.mil/stigs/os/mainframe/z_os.html

Please note that the G in STIG stands for Guide, not for Law.

Other Sources of Standards

To stay ahead of your auditors, to make your system more secure, and to make life easier, you might want to review these sources of standards from IBM:

- How to Protect System Datasets (Quick, without looking there, when you thought of system datasets to protect, did you think of the page files? HASPACE?)

  See some IBM recommendations in Appendix D "Security for System Datasets" of the RACF manual "*Security Administrators Guide*".

- What Started Tasks Should Be Trusted (Compare to what's in your DSMON.) You can see the list of started tasks which IBM says should be Trusted in the IBM manual "*MVS Initialization and Tuning Reference*" under *"Assigning the RACF Trusted Attribute*". Any started task marked TRUSTED which is not suggested by IBM is a powerful program that someone has added to your system. (By "powerful", we mean that whenever the program calls RACF to ask "Can this started task do ...?", RACF always answers: "YES, allow the access".) Your systems programming group should recognize any such started task, and likely have vendor documentation recommending that it be marked TRUSTED. (You probably want to have no started tasks marked PRIVILEGED, since that gives the same privilege as TRUSTED, but without logging to SMF.)

- What Entries IBM Gives Us in the Program Properties Table (compare to what's in your DSMON.) Any entry with a YES in your DSMON that isn't one of the ones provided by IBM is a powerful program someone added to your system. Your systems programming group should recognize it, and have some way of knowing that it is "safe".) See the standard in the IBM manual: *"MVS Initialization and Tuning Reference*" under SCHEDXX.

The Big Privilege in USS: UID Zero:

In USS (the standard UNIX included with z/OS), as with every other UNIX, users are identified by a number called the UID (for User Identifier). Any users whose UID is zero is considered to be "**Root**" or "**Superuse**r". This means that she can issue any command and do anything to any file within USS. As RACF administrator, you can control which users can have UID zero. You can give someone UID zero in the OMVS segment of her RACF user profile. Or you can permit her to the FACILITY class rule cleverly named **BPX.SUPERUSER**.

Some people believe that no person should need UID(0) all the time, and that this should be given only to certain started tasks. In that case, **BPX.SUPERUSER** can be considered comparable to a firecall id.

Why VTAMAPPL?

This is a resource class which is often not activated because no one understands it, and often no one believes that it is his job to activate it. The risk of not using **VTAMAPPL** is that some programmer could write and execute a program which gets privileges from VTAM that let it seize control of a terminal. The progarm can then, for example, paint a fake signon screen on someone's terminal in order to harvest userids and passwords. The probability of this happening may be very small. But the damage can be very big. And the way to prevent it (**VTAMAPPL**) is very easy to implement.

Why SNA Firewall?

If you use **Enterprise Extender** (ask your VTAM system programmer), you probably know that it uses a protocol called **UDP** to tunnel SNA requests between your SNA network and the SNA networks of your business partners. This means that security tools like firewalls and encryption which work on the UDP packets give no protection against the SNA messages contained in them.

Most of the time we think of VTAM as being tightly controlled, not allowing any connection unless both parties have been defined to VTAM in his control file (often named **SYS1.VTAMLST**).

However, when VTAM goes cross-network, as with **Enterprise Extender**, VTAM becomes more open-ended and flexible, allowing connections from parties he has not authenticated. In this case, VTAM resembles TCP/IP in the flexibility with which he permits unauthenticated connections. This can introduce the risk of cross-network spoofing from networks you never knew about. You can help prevent such spoofing by using the RACF resource classes **APPCLU and VTAMAPPL**. Your VTAM system programmer can help further by setting VTAM parameters (such as limiting the number of hops a message can travel from network to network.) You can see examples of possible attacks and tools to protect against them at NET-Q's website at: www.net-q.com.

Why SURROGAT?

This resource class authorizes one user to submit production batch jobs for a different userid without having to provide the password. This is perfect for your job scheduling software, to permit the userid for the job scheduler started task to submit batch jobs for userids **PAYROL**L, **SALES**, and so on. This lets you put **USER=PAYROLL** on all the payroll job cards, **USER=SALES** on all the sales job cards, and so on, without having to hardcode the password.

(If you don't put a **USER=** on the job card, then all the batch jobs inherit the userid of the job scheduling software (which for example might be **CA7USER** if the schedule sofgtware is CA7). This makes every production batch job look the same to RACF. (The userid **CA7USER** is inherited by every production batch job submitted by CA7. This makes it hard to permit only payroll jobs to payroll datasets.) With SURROGAT for the job scheduling software, you can permit the **PAYROLL** userid to all the payroll datasets, but deny access to the **SALES** userid. (Of course, **PAYROLL**, **SALES**, and all the other production batch userids should be **PROTECTED**.)

Erase-On-Scratch Starting to Roll Out

We are starting to see RACF installations with Erase-On-Scratch active. (This feature writes zeroes over a disk dataset when the dataset is erased. This prevents the next person to allocate a dataset on that part of the disk drive from being able to read the data, which could be sensitive.) This feature used to have a serious performance problem, which has since been fixed by clever changes to the hardware. With RACF you can specify this feature for selected datasets by specifying **ERASE(YES)** on the dataset rule (along with the proper **SETR setting**).

The question remains, **how do you, a smart RACF administrator, decide which datasets should have this protection**? The answer is that you shouldn't; you don't have the knowledge, nor the authority. Instead, your Legal or Compliance department, working with the application owner, should tell you which datasets are sensitive, and which regulations apply. You will then want to work with your system progarmmers to roll this feature out gradually, and only after careful testing of performance effects.

If you doubt the need to implement this feature, you might look in the RACF *System Programers Guide* under Erase on Scratch to see IBM comments.

What is z/OSMF?

This is not SMF, but rather the ***z/OS Management Facility***. This is a browser-based (think Internet Explorer, Firefox, or whatever you use, running on Windows or maybe on LINUX) management console for z/OS. It includes an **incident log**, a configuration **assistant for TCP/IP**, and tools for: **workload management**, **system and resource monitoring**, **software deployment**, **capacity planning**, and **ISPF**. This will simplify system programming tasks for new system programmers.

How do you secure it? It uses a new RACF resource class **ZMFAPLA** (with its group version **GZMFAPLA**). You will want to define RACF groups that correspond to the roles that various system progarmmers play. Ask someone in system progarmming how they would like it all set up. Resource rules in this class will have names beginning **ZOSMF**.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
October 23, 2012 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. Please see the new 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.

The Spring, 2013 meeting will also be at DTCC. We bet you know where to find the details as they become available.

For Complete Directions and to Register, Please Visit the New Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.com This website has

- Directions to both meetings
- 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 formats 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. (If you have a topic or speaker to suggest, please let us know.)

- 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**)
Dec. 3-6, 2012 in Bethesda, MD
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**)
Nov. 12-15, 2012 in Clearwater, FL
May 7-10 , 2013 (location to be determined)

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