# RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

## Our Newest Contest!!

Simon Dodge of the GARUG and SICon will be presenting at the October 9 NYRUG on **America's funniest RACF set-ups**. (All examples will be sanitized to hide the identities of the individuals and organizations involved.) You are invited to submit to Simon at **sdodge@siconsults.com** describing RACF rules, options, usage that actually happened that made you laugh when you thought about it. (One example might be the shops that had the RACF primary database on the same disk back as the back up.). We can all learn while laughing.

Most humorous entry (in Simon's opinion) may win a prize, but at a minimum will get credit in the next RACF User News (unless you ask not to be identified). No purchase necessary. You need not be part of the NYRUG to enter. Decision of the judge is final.

Please be sure to send entries to Simon, not anyone else.

## NEW YORK RUG Meeting Dates

**Tuesday, October 9, 2007 from 10AM to around 4PM**. (This is the revised, and correct date.) 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, including the tentative agenda. The meeting after that will likely be in April, 2008. Please note the NYRUG will meet twice a year from now on.

**NY Metro NaSPA Chapter (system programmers professional association) meets October 30,** 2007 in room 1219 at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM. You are warmly invited. Details inside.

------------------------------------------

**Todays Proverb** **"When you have a strong intuition, consider violating it just to see what happens. You can learn a lot of surprising things that way."**

## Vanguard Conference in Los Angeles in 2008

It's scheduled for June 1-5, 2008 in Los Angeles, CA. For details, go to www.go2vanguard.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**

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

## "I'm Bored; I've Protected All the Userids, Datasets, and CICS Transactions. Give Me Something Interesting to DO":

Pick any one of these projects, sell it to your manager, and do it: Lay out the necessary sub-tasks, so she can see how much more you do than just reset passwords.

- **Protect tape datasets completely**, including residual data, addressing the 17 character dsname in the label problem, and providing for encryption of all tapes leaving your data center. This will require you to buy lunch for the tape managment software adminsitrator. (See also the article reference on the last page of this issue.)
- **Protect USS (UNIX) files** on the mainframe.
- **Protect TCP/IP and Internet access** to your mainframe. (Issue a NETSTAT command in TSO to find out what's going on. Then buy lunch for someone in the telecomm group to learn what it means.)
- **Learn Kerberos** and consider implementing it on your mainframe with RACF
- **Learn SSL** and consider implementing it on your mainframe with RACF.
- **Clean up your RACF database**
- **Evaluate implementing Erase-on-Scratch** in RACF for selected datasets.
- JESSPOOL **protection for printouts** on the print queue
- **List all paths into the system and make sure that each is controlled** by RACF (including: NJE, RJE, TSO, started tasks, the internal reader, every applid, telnet, FTP, and other TCP/IP daemons.) This may require you to take the VTAM and JES people out to lunch.
- **Finesse your auditors** by writing down all your SETR settings and labeling it "Our Company's Standard for RACF Option Settings". Circulate it to enough people to make it official. Next time the auditors come by, give them the standard and ask them to evaluate how well you meet it.
- **Develop a program to train users in mixed case passwords** and in password phrases (but implement these only after TSO and similar programs provide needed support). Include training to make "passwords easy to remember but difficult to guess.

## On Securing FTP

Many people seem to be unaware of how many ways IBM gives us to secure FTP on the mainframe. You can use RACF to control use of IP addresses, ports, access to USS files, and a lot more. On the PERMIT command, you can permit a user to a dataset **WHEN(SERVAUTH(xx))**, allowing you for example to differentiate between IP addresses on the inside of your firewall and the outside. You can also have two copies of FTP with different security settings and permit some users to one of them and other users to the other (using the **APPL** resource class).

## A Tip on Securing SDSF

To secure SDSF with RACF, it's easier if you start by rolling out the **OPERCMDS** and **JESSPOOL** resource classes first. Then get a chart with the rules for the **SDSF** class and roll them out separately. You'll probably want to implement the **WRITER** class as well, but it's all easier if you do it one resource class at a time.

Of course, any time you activate a new resource class, such as JESSPOOL, you might want to create a batch job to execute the **SETR NOCLASSACT(classname)** for the class. Submit the batch job with **TYPRUN=HOLD** on the **JOB** card, and give operators written instructions to release the job only if there's a problem with RACF. This will provide you with "graceful fall-back", a concept familiar to novice ice-skaters.

## New York System Programmers Meet October 30 at IBM

The next meeting of the NY Metro NaSPA Chapter will be on October 30, 2007 in room 1219 at the IBM Building at 590 Madison Avenue, New York City, from 10:00 AM until 4:00 PM.

Pre-registration is requested and recommended as it simplifies getting into the building and helps us get the room set up correctly. Please RSVP to markan@us.ibm.com as soon as is possible if you are thinking of attending.

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

## The Poetry of Different Languages

Some of you may have noticed that some languages have several words for a concept that usually is covered with just a single word in another language. For example, the Eskimos are said to have several different words for different types of snow, while in English (unless you are a skier), it's all snow to you. This is supposed to reflect the Eskimo outlook on the world, and to demonstrate that snow is more important to their way of life than to ours. (Yes, I know, skiers are an exception.)

The Japanese are said to have several different words for the English word "rain", such as one word for a soft summer rain, and a different word for a heavy, crop-killing rain. (No exceptions for skiers on this one!) The Japanese also have many different words for different types of rice and for fish (depending upon the fish's size, age, and whether it is native or cultured. Mongolians have thirty or more words for different types of horse. Differences in vocabulary can reflect differences in the way people live, and in what's important to them.

The English language is said to have even more synonyms for "inebriated" than for "make love".

And of course, security administrators have different words for "give permission", such as "permit" for a RACF permission, but "grant" for a DB2 permission. Language can tell us so much about someone else's culture.

## Why You Have to Consider SSL or Kerberos or Both (the 800 Pound Gorilla in the Room We All Try to Ignore)

Many installations have most of their online users sitting at personal computers instead of the old, hardwired terminals. Users log onto the **LAN** (Local Area Network) which connects the PCs together. Once logged onto the LAN, they log onto the mainframe through the LAN. Since the architecture of a LAN sends every message to every workstation on the LAN, each user's signon stream (mainframe userid and password) travels to every PC on the LAN (or at least on the sub-net, or up to the first switch or router).

This means that any computer on the LAN can see every userid and password as they go by. To see this, you need a type of program called a **sniffer**. Sniffer programs can be downloaded for free over the Internet. They execute on a personal computer and read every message that goes by on the LAN. You can even specify filters, so they only pay attention to messages that contain the words: login, userid, or password. This makes it easy to learn someone else's mainframe userid and password, if you can get access to the LAN cable. (Good thing the security guards in our lobby only allow honest people into our building.)

If you don't believe this, you can try it out. (But don't do this without getting your manager to approve the experiment first. Many people get upset when you demonstrate that there is a gorilla in the room.) Get a laptop and download a sniffer over the Internet. Walk into your manager's office, pull the ethernet cable out of his desktop computer, and plug it into your laptop. Start the sniffer running on the laptop and see the read the messages from other workstations as they go by. Disconnect as soon as you have proved the point, and before you see anything compromising.

Encrypting your userid and password won't protect against sniffers, since all they have to do is record the encrypted message and play it back without decrypting it.

Two approaches will protect against sniffers: Kerberos and **SSL** (Secure Sockets Layer, currently being supplanted by its successor **TLS** or Transport Layer Security). Not all programs such as **TSO** and **CICS** support both of these thoroughly yet, but RACF and TCP/IP do. Deciding which one is best in your organization and getting people to work together to implement it would be a good way to fight boredom.

## RACF 1.9 vs RACF 1.9

Some of you may remember when the first RACF release 1.9 came out about a decade ago. It had so many new features that one IBMer said "We'll never put that much new stuff into a single release ever again." That release had support for JESSPOOL, OPERCMDS, B1 security, tokens, VERIFYX, a new blocksize for the RACF database, and a slew of performance improvements (including elimination of the CONNECT record from the RACF database).

Now IBM has again release a new RACF 1.9, but this of course is part of a different number scheme (sort of like Fahrenheit and Celsius). This is "Secureway Security Server for z/OS 1.9", but some of us just think of it as the "new 1.9".

This release is remarkable for the small number of new features, and the large number of improvements in the manuals to make them easier to read and more useful. Most of the new enhancements have to do with digital certificates and **PKI** (Public Key Infrastructure).

## Getting the Authority to Keep Unsafe Software Off the System (a comment from the RACF-L List Server)

One lister mentioned that he had been charged with evaluating software packages for password resets. And that one package he was being encouraged to consider required several different types of privileges, including supervisor state and RACF SPECIAL. He didn’t know how to be able to trust this software, that is to know that it wouldn’t introduce security exposures to his system. The following (slightly edited) posting provides one technique:

“One way to approach this is to request from any vendor of software that needs User SVCs (or any other means of obtaining supervisor state) a software integrity statement comparable to IBM's (stating that, properly installed, the software product won't make it possible for unauthorized programs or users to obtain supervisor state). Ask for the vendor to provide it on company letterhead, signed by a senior executive. Most won't sign it without advice from a lawyer, who won't bless it without talking to the developer.

Some vendors have re-written user SVCs, APF authorized programs, and other “back-doors to securty” to make them be safe. They do this order to be able to provide an integrity statement comparable to IBM's. It is pressure from customers that encourages vendors to do this. If they have questions, refer them to the techniques documented in IBM's manual: **Assembler Language Authorized Programming Guide** and to the references to IBM's integrity statement there. You could even ask them for an independent evaluation (some consultant who would sign an NDA (Non-Disclosure Agreement) and give a formal evaluation in the light of the issues and techniques in that manual).

This poster doesn’t do such evaluations, but there are consultants out there who might. Peter Goldis comes to mind. If they won't give you a software integrity statement on company letterhead, then why would you be willing to install their software on the computer you pay IBM millions of dollars for, for which IBM does give you an integrity statement?”

In fact, some organizations make it part of their software acquisition procedures to request a software integrity statement from all vendors. You don’t always get it, but if you don’t ask for it, then you are sure not to get it. And the vendor won’t feel the pressure to follow sound programming practices.

If you don’t ask for it, then how could your management sign off that they know the controls protecting information on the computer can be relied upon?

## HG RACF and Security 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 "How to Audit ..." classes above.)

1) HG04 **Effective RACF Administration** (**$1995**)
**Sept. 17-20, 2007 in Vienna, VA**
**Feb. 26-29, 2008 in Clearwater, FL**
**Sept. 15-18, 2008 in Raleigh, NC**

2) HG05 **Advanced RACF Administration (\$1990)**
**March 3-6, 2008 in Clearwater, FL**

3) HG06 **UNIX (USS) for RACF Administrators** (**$490**)
**May 19, 2008 in Bethesda, MD**

## HG How To 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 and Security" classes below.)

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$1550 and 3 days in 2007, $1980 and 4 days in 2008**)
**Nov. 14-16, 2007 in Clearwater, FL**
**May 5-9, 2008 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.) ($1560)**
**May 20-22, 2008 in Bethesda, MD**

## NYRUG (New York RACF Users Group):

Our next meeting is at IBM, 590 Madison Avenue. Attendees **must present a government issued photo ID** to enter the building. Admission is free to hear these great speakers, but you must pre-register by emailing NO LATER THAN NOON October 5, 2007 to Mark Nelson (markan@us.ibm.com) with "NYRUG MEET" in the subject line and your name and company in the body. Pre-registration is highly recommended.

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/XNEWSTXT.HTM#nyrugref .**

Starting roughly at 10AM (tentative agenda) ending around 4PM, and in no predictable order:

1. Simon Dodge will speak on America’s Funniest RACF Setups (Please note contest described on page one of this issue.)

2. Eric Rosenfeld of IBM will speak on “Introduction to Kerberos on z/OS”

3. Stu Henderson will speak on “Kerberos Implementation”

4. A great speaker from IBM on some critical topic

(Please note that times are approximate and that speakers and topics are subject to revision.)

Time: **October 9 (revised date), 2007 from 10AM to around 4PM**
Place: **IBM, 590 Madison Avenue**. Attendees must present a photo ID to enter the building and must pre-register in advance.

## A Tip On Implementing Role Based Security Administration:

Role Based Administration has you pre-define roles, which correspond to collections of privileges. It makes perfect sense to use RACF groups to represent roles. Some auditors have been pushing us in this direction. Some RACF administrators would like to implement this, since it greatly simplifies RACF administration. While Sarbanes-Oxley doesn’t require it, it’s easier for management to sign off on the controls if you use Role Based Admin.

The only problem is that many of us inherited a mess. Getting from Mess to RBA can seem a daunting task.

The simplest way to accomplish this is to build a new set of groups corresponding to roles, and then permit these groups to the datasets and resources that have been approved. This is building a new infrastructure while leaving the old infrastructure intact (for the time being). The new infrastructure should have no effect on the old. (If you can’t get someone to agree on what the groups and roles should be, then don’t waste your time, since it’s almost impossible to succeed if you’re doing it all alone.) Then gradually and carefully move users to the new infrastructure and decide when to delete the old. You might have a naming convention to identify the groups which are part of the new infrastructure.

## .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** .

**The RACF User News** is published two times a year (March and September) 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/

# IBM 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**

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.