RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 73):

IBM Offers White Paper on SNA Security

The following link will take you to a great introduction to some of the issues regarding SNA security and how to deal with them. It is titled:

'**Securing an SNA Environment for the 21st century**'

http://www-1.ibm.com/support/docview.wss?rs=852&uid=swg27013237

For further info and case studies, you might take a look at:

http://www.net-q.com

Article on Supervisor Call Integrity Now Available:

It is titled "**SVC's: Analysis for Integrity and Audit**". If you are addressing MVS security, as a system programmer, security administrator, or auditor, this will give you insight into how one of the common "backdoors" to MVS security can be addressed. It is at:

http://www.goldisconsulting.com/SVC.swf

NEW YORK RUG Meeting Dates

Thursday, October 30, 2008 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, including the tentative agenda. The meeting after that will likely be in Spring of 2009. Please note the NYRUG will meet either 2 or 3 times a year from now on.

NY Metro NaSPA Chapter (system programmers professional association) meets

on Wednesday Nov. 5, 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.

Vanguard Conference in Los Angeles in 2008

It's scheduled for May 31-June 4, 2009 in Jacksonville. FL. For details, go to www.go2vanguard.com .

Today's Quotation

"We cannot direct the wind, but we can adjust the sails."

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 for z/OS 1.10 has more great features:

1. User defined fields in the USER and GROUP records. (While there is an earlier method of adding installation-specific fields to RACF profiles, it required assembler language programming, and is generally considered difficult to administer. This new way will be much easier.) To define a new field in the user or group records in your installation, use the **CFIELD** (customized field) resource class in RACF. Names of rules in this class have the form **USER.CSDATA.fieldname** or **GROUP.CSDATA.fieldname**. This lets you use the new fields in ADDUSER, ALTUSER, ADDGROUP, and ALTGROUP. Experience suggests that you want to control tightly who can approve the addition of new fields this way, how they are defined, and how many new fields you create.

2. New ways to delegate authority over userids. For example, new **FACILITY** class rules named I**RR.LU.TREE,owne**r **IRR.LU.TREE.OWNER.owner**, and **IRR.LU.TREE.EXCLUDE.userid**, let you delegate the authority to issue LU commands just for certain parts of the RACF group tree (which of course is described in the DSMON report). Additional FACILITY rules named: **IRR.PASSWORD.RESET**, **IRR.PWRESET.OWNER.owner**, **IRR.PWRESET.TREE.owner,** and **IRR.PWRESET.EXLCUDE.userid** let you delegate authority over the resetting of passwords (a great way to set up your Help Desk).

3. With the z/OS Health Checker, you can now define your own RACF checks, using the **RACFHC** resource class.

Here's a Great Idea for Disaster Recovery

The **GDPS** (Geographically Dispersed Parallel Sysplex) makes it possible to extend a sysplex to another location (such as your recovery hot-site). This lets you have instantaneous backup of critical datasets immediately available at the hot-site. Would it make sense to include the RACF database in this scheme?

What To Do About the New Password Options (and the One Critical Element Many Installations Miss):

IBM has given us several new RACF features for strengthening new passwords:

- Mixed case (upper and lower case) passwords and requirements
- Pass Phrases (like passwords, but length 14 to 100)
- Changes to RACF exit named **ICHPWX11** to permit pass phrases of length 9 to 100 (instead of 14 to 100)

Many of these relate to requirements from auditors and others to make passwords harder for a hacker to guess. Some of these requirements have been blindly insisted upon by people who are familiar only with AS/400 or Windows or UNIX.

We need to be careful how we roll out these new RACF features, for several reasons:

- They will require training of users, and we will likely have only one chance

to get it right

- Some other software may not be ready yet (but soon will be)
- The standards other people try to impose on us may change, or may turn out to be invalid
- The one critical element many installations miss (described below).

Training of users will be a major effort. If we do it clumsily, users will view it as just another stupid difficulty imposed on them by the folks from IT. If we show them easy ways to come up with new passwords, and why password strength is important, there will be fewer requests to the Help Desk for password resets.

Some other software (TSO and CICS come to mind) will not be ready to handle mixed case passwords, nor password phrases until a later release. If an auditor reads that RACF supports them, and then suggests that we should implement them right away, we will need to explain to the auditor that RACF support is not sufficient to be able to implement these. There would be serious problems if we permitted lower case characters in RACF for example before TSO upgrades its sign-on screen to support lower case. That will not happen until release 1.10 of z/OS, which is not available until the Fall of 2008, and which system programming does not intend to implement until six or more months after that. We may have other software with signon screens that is not yet capable of accepting lower case password characters or password phrases.

(This raises the fascinating question of who is responsible for determining whether all **applids** (programs with signon screens) are ready to accept these new RACF features. The default (as with so many things in life) is that it's the RACF administrator's fault if we implement a new RACF feature and it blows up because some other piece software couldn't handle the new feature. In the case of password options, the VTAM system programmer would be a good source to learn the names of all the programs that have signon screens.)

In some installations, auditors or others have tried to enforce password standards from other platforms onto the mainframe. These people may or may not have the actual authority to do so. Standards that are really just one person's opinion are subject to change, and subject to being overridden by wiser heads. The best arrangement is to have an official, enterprise-wide standard specifying what password length and content rules are acceptable. Then everyone has a single, straight-forward standard to meet.

The one critical element that many installations may miss is: ***Restrictions on password length and content have almost no importance if users are not properly trained***. If for example, you decide to have no vowels allowed in passwords, users (and hackers) will know this. Since it will be easier for hackers who know the (publicly stated) restriction, they will have fewer combinations of letters to select from. If you make a list of restricted words which are not permitted in passwords, users will select variations of words to bypass the list. Users will still write passwords down or make them easily guessable, unless you the train your users.

These new password options are an opportunity to put on an effective training program, one which helps users to understand the purpose of hard-to-guess passwords, and one which changes their behaviour to support this purpose.

In summary, as the new password options become available, we need to:

1. Determine as far as possible an enterprise-wide standard for password length and content.

2. Decide whether to change RACF exit ICHPWX11 to permit password phrases of length 9 to 100 (instead of the default 14 to 100).

3. Learn the names of all applids (programs which have signon screens) and make sure that they are ready to handle mixed case passwords and password phrases.

4. Train the Help Desk and anyone else involved in resetting passwords

5. Consider single-sign-on tools. New ones are coming on the market. Existing ones such as Kerberos are already available for free with Windows, UNIX, Novell, and RACF, and may soon be supported by all programs with signon screens.

6. Develop a training program to teach users how to make passwords that are easy to remember but difficult to guess. User won't remember the new passwords they set unless we show them a method that makes them stop and think about what the new password will. Showing them an easy formula that hackers can't guess will help this.

7. Measure the effects of your training program by plotting the number of invalid passwords entered over time, both before and after your training program.

Below is a sample SAS program to list all the instances of invalid passwords. Adding code to make it count the number of violations, and then to plot this value over time should be easy for you to do..

```
DATA A;
  KEEP      USERID EVENT QUAL DATE TIME HOUR MIN;
  FORMAT DATE YYMMDD.   TIME TIME.;
  INFILE SMFIN;
  INPUT @2 REC_TYPE    PIB1.  @;
  IF REC_TYPE NE 80 THEN DELETE;
  INPUT  @3    DATETIME      SMFSTAMP8.
        @15   SMF80DES      PIB1.
        @17   EVENT         PIB1.
        @18   QUAL          PIB1.
        @19   USERID         $8.
        @27   GROUP          $8.
        @;
* EVENT IS 0 FOR SIGNON (PASSWORD CHECK);
* QUAL IS 0 FOR BAD PSWD AND IS 36 FOR BAD PASSWORD PHRASE;
   IF EVENT NE 0            THEN DELETE;
   IF QUAL   NE 1 AND QUAL NE 36 THEN DELETE;
   TIME = TIMEPART(DATETIME);  DATE = DATEPART(DATETIME);
   MIN = MINUTE(TIME);  HOUR = HOUR(TIME);

PROC SORT ; BY DATA TIME;
PROC PRINT;
```

(Note all SAS statements end in a semicolon and any line with an asterisk in column one is a comment. The DATA section reads the SMF data and writes it to a SAS file

named A. Then the PROC statements use the SAS file as input. The DATA statement says "Create a SAS file named A." The KEEP statement names the fields to be included in the SAS file. The INFILE statement gives the DDNAME of the input SMF file. INPUT @2 reads from position 2 the numeric record type of the SMF record. For more details, please see issue 65 of this newsletter.)

I'm Still Bored, Can't You Tell Me Some Things I Can Do To Know That My Networks are All Secure?

Yes, start by recognizing that you have both SNA and TCP/IP networks connected to your mainframe, and that neither one is going away soon. (You may be using Enterprise Extender and OSA (Open Systems Adaptor), but there is still SNA tunneling inside TCP/IP or inside UDP/IP. All the TCP/IP security tools such as encryption, SSL, and firewalls won't protect against SNA attacks if the tools are applied only to the envelopes, and not to the actual SNA inside the envelopes.)

Identify all the paths into your system. These will include:

- **TSO, NJE, RJE**
- **CICS**, **IMS**, and all the other programs with signon screens
- **USS** (UNIX System Services)
- **FTP**, **Telnet**, and all the TCP/IP daemons (use the **TSO** command **NETSTAT** to identify them all. Don't be surprised if you see **DB2**, **MQ Series**, or **CICS**.)
- Recognize that FTP can allow submission of batch files, access to DB2, and access to print files on the spool
- Recognize that telnet can permit access to TSO, CICS and other applids
- Make use of the **SERVAUTH** resource class in RACF and the **Policy Agent** software that provides firewall-like functions including Intrusion Detection.
- Get Windows administrators to implement Kerberos on AD (or to take other measures) to protect against hackers with sniffer programs learning mainframe userids and passwords.

Interesting Products Column:

While we have not tested any of these products, we think you might want to take a look at them:

- **PWCHECK-PRO** is a password quality audit tool for RACF security administrators and auditors. It is designed to help detect trivial or poorly chosen passwords, passwords that are weakly encrypted, or cleartext passwords that might reside in memory. For more info: www.goldisconsulting.com or phone (617) 229-5136.

- **APFCHECK** answers what some consider the most important question to answer in reviewing MVS integrity: 'Which userids have more than READ access to even one APF library?' taking into account access based on privileges such as OPERATIONS, Global Access Checking, Warning Mode, ID(*) specifications, group memberships and so on. For more info: www.goldisconsulting.com or phone (617) 229-5136.

- **Rocket Strong Authentication Expert** for z/OS (http://www.rs.com/portfolio/strong) is a strong, two-factor authentication solution for z/OS. For more info phone: 617-614-2301.

- **Rocket LDAP Bridge** (http://www.rs.com/portfolio/ldapbridge) links non-mainframe directories and applications to your mainframe data sources and bi-directional password synchronization between mainframe security database and the client and updates between multiple mainframe security data sources (e.g., RACF, CA-ACF2, CA-TSS). For more info phone: 617-614-2301.

NYRUG (New York RACF Users Group):

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 to hear these great speakers, but 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 and contact info. **YOU WILL NOT BE ADMITTED UNLESS YOU HAVE PRE-REGISTERED DUE TO SECURITY REQUIREMENTS AT THE HOST SITE, even if you have pre-registered for previous meetings.**

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. Use of custom fields in the RACF database
2. Update on RACF 1.10
3. New RACF features in Health Checker
4. Details of RACLIST
5. Mining the RACF Database with Access and DB2

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

Time: **October 30, 2008 from 10AM to around 4PM**
Place: **DTCC, 55 Water St, NYC (about as far south as you can get in Manhattan)**. Attendees must present a photo ID to enter the building and must pre-register in advance and be prepared to go through a security scanner.

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 70 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..

For complete directions, please go to: www.stuhenderson.com/NYCRUG1.pdf Or to: www.stuhenderson.com/TampaRUG1.pdf which should be available shortly.

New York System Programmers Meet at IBM

The next meeting of the NY Metro NaSPA Chapter will be at the IBM Building at 590 Madison Avenue, New York City on Wed. Nov. 5.

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.)

1) HG04 **Effective RACF Administration** (**$1995**)
Sept. 15-18, 2008 in Raleigh, NC
Feb. 24-27, 2009 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($1990)**
March 31-April 3, 2009 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$510**)
June 8, 2009 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**)
Nov. 17-20, 2008 in Clearwater, FL
May 4-7, 2009 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)
June 9-11, 2009 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** .

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 donMt 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