RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 69):

RACF Now Supports PassPhrases:
The latest release of RACF now lets users identify themselves by typing in a passphrase instead of a password. (Userids must be defined with a password in order to support a passphrase.) This is an excellent opportunity to train your users in how to make passwords and passphrases "easy to remember and difficult to guess". Don't implement until all MVS images sharing the RACF database are on the correct level of RACF. Don't let this be implemented without putting on a training program for users.

Remember Vanguard's estimate that each password reset costs a company at least $60. (Contact Vanguard for details and exact dollar figure.)

Do you know the trend of password reset frequency each week? Why not start plotting it now, so you can see the improvement when you put on your training program? You can collect the information from SMF data, and SAS is a great tool to plot it.

It is considered a "best practice" by all the experts that the RACF administrators should split a bonus each week of the dollar value of any reduction in password resets.

Here is the syntax to add a passphrase to a user record:

ALU USER02 + PHRASE('July14IsBastilleDayLikeJuly4, ButInFrance')

NEW YORK RUG Meeting Dates

Thursday, October 26, 2006 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 April, 2007 Please note the NYRUG will meet twice a year from now on.

Todays Proverb "You always hurt the one you love when the one you love is you."

Vanguard Conference in St. Louis in 2007
It's scheduled for June 10-14, 2007 in St. Louis, MO. For details, go to www.go2vanguard.com .

IMS Security Adminstrators Rejoice!
The latest release of IMS now always calls RACF and the SMU becomes obsolete. This makes IMS more like CICS, in that it generally calls RACF all the time to get security answers. You may need to buy your IMS admin lunch.

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 Protection of the Hardware Configuration Definitions

Many of us have wondered how the hardware configuration is defined, for example what LPARs exist, what they are named, and what disk packs are shared across LPARs and CPUs. This can be important to us, since we need to be aware of situations like this: Imagine two LPARs (and thus two copies of MVS, and of the RACF software) each with its own RACF database. Maybe one LPAR is TEST and the other is PROD. Imagine the production accounts payable master file is on a disk pack shared by the two LPARs. If we pay attention just to the RACF database on PROD, we might miss the possiblity that the RACF database on TEST has completely different rules protecting this master file. This could make it possible for users on TEST to update this file improperly.

So it's useful for RACF administrators (and auditors) to know what the Hardware Configuation is. And of course we need to protect the HCD itself from unauthorized updates. **Mark Hahn** sends us this article describing how to protect the HCD with RACF:

The HCD (Hardware Configuration Definitions) is the blueprint of your z/OS System. It grew out of two programs: the **MVSCP** (MVS Configuration Program) which defined the hardware to MVS and the **IOCP** which defined the hardware to the channel Subsystem. The two programs were separate entities and their settings were not cross-checked for consistency before becoming the active blueprints at an IPL. As you can imagine, inconsistencies did occur and were frequently discovered at very inconvenient times.

Now there is the **HCD**, an ISPF panel-based service used which builds the input/output definition file (**IODF**). The IODF has almost the entire configuration of multiple processors within multiple partitions all packaged together. This one program manages all of the configuration data. This data includes all device definitions, how the devices may (or may not) be shared between partitions, the esoteric device name table, channel (types) to control unit to device mappings and much more.

There are several steps involved in the successful generation of an IODF and its **IOCDS**. The panels step the user through the definition of hardware environment. A WORK IODF can be built before the production version is defined. Activation with TEST allows validation of the built IODF against the live running system. HCD can also build a **CONFIGxx** parmlib member for the local system or systems within a sysplex. All of these functions can profoundly affect your systems. This data is hardly something that should be readily accessible to every user on your system. This is where the RACF steps in with its relevant profiles and control options.

RACF within z/OS provides multiple layers of control, as you'd expect.

The user accessing the IODF data sets must have appropriate permission to read or update the IODF dataset through the relevant **DATASET profiles**.
The **IOSAS** address space also must also have read authorization to the IODF data set if the MVS operator command **ACTIVATE IODF=xx** is issued. This dataset authorization can be provided by the dataset UACC, an appropriate PERMIT command, its STARTED class profile or via an entry in the Program Properties Table.
The **MVS ACTIVATE command** can be controlled via an **OPERCMD**S profile (MVS.ACTIVATE). There are two levels of access:
READ – only allows activation with the TEST option
UPDATE – allows the user to activate a change
Additionally an **OPERCMDS** profile for MVS.DISPLAY.IOS can be defined if the user is to process a CONFIG command from a sysplex member to view the actual configuration.

(Cont'd)

(Cont'd)

The HCD service itself has two possible calls for **FACILITY** class profiles, both utilizing the prefix **'CBD'**:

- **CBD.CPC.IPLPARM** – determines who is allowed to review (READ access) and/or change (UPDATE access) the next IPLPARM and IPLADDR values. Another level of access (NONE) is in effect if the user is to have no access to the values, or if the CBD.CPC.IOCDS profile is not defined. These two parameters (IPLPARM and IPLADDR) affect the specifics of the next system IPL. They can also be specified at the hardware console if preferred.
- **CBD.CPC.IOCDS** – controls access to local IOCDS functions. If this profile is not defined, the operator is asked to authorize the IOCDS update request. READ access to the profile permits the user to query the IOCDS for information contained therein. UPDATE access allows the user to update an IOCDS (using either IOCP or HCD), or to review / change IOCDS control information.

When researching the use of IODF datasets, one must remember to consider the accompanying **LOADxx** member of SYSn.IPLPARM or SYS1.PARMLIB on the IODF volume. The IODF statement within the LOADxx member further defines the IODF parameters to be used for the IPL in progress.

It should now be apparent that there are extensive controls available to protect one of the more powerful functions within z/OS: that of defining your hardware environment. Hopefully now you can determine which controls and protections are appropriate for your environment.

The primary reference for this article was the **Hardware Configuration Definition User's Guide (SC33-7988-05**).

Mark S Hahn is a mainfame computer security author and consultant based in Southern California. His website can be found at www.mhahnbe.com .

Results of Exciting Quiz on How to Bypass RACF:

Last issue we provided a list of twelve ways to bypass RACF, and offered an exciting quiz to see who could describe additional ways. (Back issues, including the list of ways, are available online at www.stuhenderson.com.) The winners of the contest are:

1. **Nigel Pentland** of Scotland whose webpage is referenced on the last page of this issue
2. **Leslie Wagner** of New York
3. **Gunnar Myhre** of North Carolina
4. **Steve Smith** of New Jersey
5. **Jim Yurek** of Texas

These winners should be proud, both of their technical knowledge and the speed with which they submitted their answers. (Other contestants submitted good answers, but only the first five to respond are winners.) Each winner receives a handsome black canvas briefcase.

Of course, you want to know what additional ways they provided to bypass RACF. Here they are:

13. Have update access to an APF library, write a program to give myself protect key zero and then to modify my ACEE control block in memory (built by RACF when I signed on) to give myself OPERATIONS. Move the program into the APF library and execute it.

14. Have update access to an APF library and move one of my own programs into the library with the **same name as a program in the PPT which bypasses RACF**.

15. Access a dataset on shared DASD from a different LPAR with a different RACF database, or even from a different operating system running in a different LPAR (Honorable mention goes to **Robert Gwirtzman** of New York for this)

16. Have READ access to a SURROGAT profile for a userid which does have access to the dataset

17. Have access to the info in a dump when an authorized job abends

18. Physical report output is not controlled or SDSF access is not granular enough

19. Code a RACHECK pre or post exit to allow the access

20. Code the RACF Dataset Naming Convention table to switch all input dataset name HLQs to your userid HLQ

21. Have access to the RACF database and use the Block Update Utility to modify a dataset rule to give myself access. (This is Jim Yurek's "personal first choice". Have the auditors checked what type of car Jim drives?)

22. Use a RACF password cracker program (needs READ access to the RACF database)

23. Call the Help Desk, impersonating an authorized user, and ask to have your password reset.

Congratulations to all the winners! And thanks for sharing your knowledge.

Please note that all these techniques do not mean that RACF has holes or that MVS security is weak. These all result from someone not implementing properly the tools IBM gives us to secure the system. When the tools are properly implemented, MVS is considered to have no ways that its security can be broken if the security is implemented properly (unlike some other operating systems.)

DB2 Internal Security to RACF Conversion Notes:

- RACF makes security administration easier than DB2 internal security because RACF allows the **use of wildcard characters** (asterisk and percent sign) in the names of the rules. A good starting point to developing your conversion plan would be to list all the DB2 tables, views, databases, plans, etc in alphabetic order. (Your DBA can do this easily.) Then see which ones have similar names and similar access permissions, in order to determine which ones could be covered with generic rules. Your DBA will be amazed at how simple life can be.

- RACF also make administration easier because it avoids the "**cascading revoke**" feature of DB2 internal security administration.

- While IBM provides us with a utility to convert DB2 internal security tables to RACF rules, many installations have found that using this tool just converts DB2 garbage to RACF garbage. Start by identifying the owners of the data (if the DBA hasn't already done this) and then getting the owners to tell you what the accesses should be.

- The RACF exit for DB2 makes it easy to roll out RACF security gradually, since it reverts back to the DB2 internal security anytime a RACF class for DB2 is not active, or has no matching rule. Plan your implementation to go one resource class at a time. Throw a big party after each resource class is successfully implemented.

- The RACF exit for DB2 caches decisions it gets from RACF, that is, it saves the answer from a RACF call so it doesn't have to call RACF again when the same question comes up again. This can be sticky when you change a RACF rule, since the cached decision doesn't get updated when you update the rule. The solution is to tell DB2 to call RACF again to update the cache. You can solve this by using the DB2 DROP command, as described in the conversion guide.**RACF Access Control Module Guide**, SC18-7433-02.

- Before you convert, you have to decide which naming convention to use for DB2 resource classes, the IBM standard names or the tailored names. Each DB2 subsytem is identified with an up-to-four character sub-system name, such as **DB2T** or **DB2P**. (These names are specified in an **IEFSSNxx** member of parmlib.) Depending on which naming convention you choose, the sub-system name will be part of either the name of the rule (IBM standard names) or the name of the resource class (tailored names).

  When you make this decision, please keep in mind that if you later make the DB2 database part of a storage group (as part of a parallel sysplex), the name of the storage group will be used to replace the name of the sub-system id. This might cause you to rename your resource classes, or to recreate all your rules.

  One possible way to ease this works only with the IBM standard resource class names. You define a **RACFVARS** class rule to provide a substitution value in the name of the DB2 resource rules. Set the value of this variable to be the sub-system name, and later if you need to change it to the value of the sysplex storage group.

- One issue facing CICS installations is how to deal with the identity of the user passed from CICS to DB2. This can be several different values, such as the RACF userid of the user or the userid of the CICS region, or other values. This value is set as AUTHID or AUTHTYPE by the CICS system programmer for each transaction that uses DB2. Possible values include: **USERID** (of the user signed on), **GROUP** (of the user signed on), **OPID**, **TERM** (term id), **TX** (transaction id), and **SIGN** (SIGNID from DB2CONN) or a string of characters. The ACEE (RACF user definition) of the user signed on to CICS is passed to DB2 only if the value is either USERID or GROUP.

- Depending upon how this option is set for each CICS transaction, this can cause difficulties in the conversion.

- **Dave Noveske** passes on this Conversion Gotcha:

No current or planned release of CICS supports DB2Entry **AUTHTYPE(REGIONID**) using RACF for DB2 Security. It only supports USERID or GROUP.

We recently discovered how DB2Entry AUTHTYPE(REGIONID) processes, we find that we would have to maintain dual security in RACF and in DB2 since the ACEE is not passed from CICS to DB2.

If order to validate if you have 100% conversion to external (RACF) security from DB2 internal security try to remove what should be obsolete DB2 internal security tables as a part of your conversion testing plan

- **Janie Small**, an independent consultant based in Florida, suggested one work-around to this problem, which she has used successfully: Define all transactions in CICS that utilize DB2 to use list of groups. In DB2, the transactions are given authorization to plans and of course, transactions for RACF are not defined as users or groups. For this conversion, after we changed the CICS side, the groups were then put in the access lists for the DB2 plan privileges needed. Obtain a copy of the book **CICS DB2 Guide, CICS Transaction Server for OS/390, SC33-1939.** A search on the manual number on the internet will provide a copy.

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**)
Nov. 1-3, 2006 in Clearwater, FL
May 7-9, 2007 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)
Dec. 11-13 2006 in Bethesda, MD

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**)
Feb. 27-March 2, 2007 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($1990)**
March 5-8, 2007 in Clearwater, FL

3) HG17 **Comprehensive z/OS Security (Formerly: How to Be an Effective z/OS or OS/390 (MVS) Data Security Officer**) (covers CICS, VTAM, DB2, and JES security along with MVS security, SAF, OS/390, and z/OS) (**$1290**)
Dec. 6-8, 2006 in Vienna, VA

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 NOONOCTOBER 24, 2006 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:

- User Data Practical Applications **(Simon Dodge**, Sicon)
- RACF 1.8 Update (IBM)
- The Unadulterated History of RACF (30th Birthday pary!) (**Mark Nelson**, IBM)
- PKI (Public Key Infrastructure) (**Wai Choi**, IBM)
- IRREVX01 (**Simon Dodge**, Sicon)

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

Time: **October 26, 2006 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.

Interesting Products Column These are products which we think you will find interesting, but you should perform your own evaluation before deciding whether to use.

- EKC has several software tools for RACF administrators and auditors. These include tools to report on the RACF database, to help clean it up, to provide support for firecall ids, and password resetting. For more info, please see www.ekcinc.com .

- NewEra Software offers their **FOCUS Control Environment** software which detects, evaluates, documents, and reports on changes made to critical system components through a unique inspection process. For more info please see www.newera.com .

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**