RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 79):

This Issue's Themes:

- Securing New Types of Connections
- What to Do When...

Another Great Source of Free, Practical Info:

Here's a Redbook on Identity Propagation, describing how to link security on mainframes to that on distributed systems like Windows and UNIX , co-authored by the famous Simon Dodge. To get a free PDF copy of "***End to End Security - z/OS Identity Propagation"***, click on

www.redbooks.ibm.com/redpieces/abstracts/sg247850.html?Open

or go to www.redbooks.ibm.com and enter the following order number in the SEARCH box: ***SG24-7850-00***

Here's a Link to the Stinkin' Operations Presentation:

You've probably heard about the "***You Don't Need No Stinkin' OPERATIONS***!" presentation. Here's where to find it:

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/r99_dont_need_operations_for_dfdss.pdf

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, November 1, 2011 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 and new website.,

(The meeting after that will be **a Spring date to be determined in 2012**)

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!

Today's Quotation

"***A manager's (RACF administrator's) biggest challenge is to know what information she needs, and then to find the people who owe her that information.***"

— With apologies to Peter Drucker (Think of the Compliance Department and the VTAM system programmer, and the auditor)

Backgrounder on RACF Identity Propagatation

Here's a little background to get you ready for Identity Propagation. Each of your users has a RACF userid.

Each user might also be identified by a different type of name, the kind of name that Active Directory uses with Windows, the same type used by LDAP. This type of name is called a DN or Distinguished Name. It's the kind of name that says O=organization name; OU=zoneName; OU=divisionName; OU=deptName; CN=commonName (such as John Smith).

Users who log onto Windows in order to log onto the mainframe have to prove who they are twice: once to Windows and then to RACF. Wouldn't it be nice if someone could invent a way to map or translate one of these names to the other? IBM has, and the feature is called Identity Propagation. Does this make you think of Single Signon?

Get ready to learn about RACF Identity Propagation from Simon Dodge of the Georgia RACF Users Group, and also of Wells Fargo Bank. Simon just finished a residency with IBM in Poughkeepsie studying Identity Propagtion and co-authored a Red Book on the subject (described on page 1). He will fill us all in at the NYRUG meeting November 1.

An Expedited Way to Deal with Auditors

Auditors often ask the same questions every year from their checklists and formal procedures. Wouldn't it be great to be able to demonstrate to them automatic checks you've installed that verify the information they are asking for? And let them collect it themselves through SDSF? You've got this already for free with IBM's Heatlh Checker for z/OS. Here are some of the checks you can install, and then use SDSF to give the auditors the ability to review it all on their own:

- IBMUSER is revoked
- Critcal resource classes are active
- Sensitive datasets are properly protected
- The Authorized Caller Table has no entries
- Other checks that you define

This has the added advantage that it lets you show the auditors that you have an automated checking system in place, and that any alerts raised can be immediate and can be routed to someone other than the system programmers.

Health Checker is easy to set up, working with your system programmer. You will find it is more useful to you than it is to the auditor. Here's where to learn more:

http://publibz.boulder.ibm.com/epubs/pdf/e0z2l160.pdf and

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/gse_2009_11_racf_health_checks.pdf

RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

Little Known Connections You Will Want to Secure

Several types of mainframe computer connection introduce new security risk and/or capability. You want to be familiar with the following terms, the risks each introduces, and how to investigate them further.

- **LPARs or Logical Partitions**. This is virtualization in the hardware, letting one CPU pretend to be two or more CPUs, each with its own copy of MVS, and each with its own copy of the RACF software. They may share a common RACF database or each have its own distinct RACF database. If the LPARs have shared DASD (disk packs they can all access), and if you have distinct RACF databases, you may need to coordinate changes between the RACF databases. In effect, you have physical access to the disk pack from two different systems, each with its own set of logical access rules. To learn what LPARs you have, and what shared devices you have between them, you can learn HCD (the Hardware Configuration Definition file) from your system programmer and then browse the IODF (Input Output Definition Files). Another approach is to use software such as ***StepOne*** from New Era Software (www.newera.com) with a free 30 day trial at (http://www.newera-help.com/StepOne-Download.html)

- **Sysplexes** which consist of several CPUs connected by fiber optic cable, with gigantic storage boxes called Coupling Facilities. Imagine two CPUs in the same sysplex, each with its own copy of MVS and its own copy of DB2. Each DB2 instance has its own copy of some database. The system programmer has defined the two DB2 databases to the sysplex in a way that causes changes in one of them to be mirrored in the other. If you are using RACF to secure DB2, and if each of the two MVS images has its own RACF database, you can see the risk. A change in one copy of the DB2 database would be subject to the RACF rules in that database, and would be automatically reflected in the other DB2 database. The RACF rules for the other database might disallow the change, but the change would occur anyhow, without the RACF administrator being aware. Now imagine that instead of DB2 databases, you are mirroring copies of the RACF database, or of any VSAM file. You want to know what sysplexes are defined in your datacenter, and what datasets are being mirrored across them. Use the same tools to learn about LPARs described above to learn about sysplexes and mirrored datasets.

- **the Internet** involves not only exposing your system to many more users; it also adds to the ways that security is implemented. For example with several Internet programs such as FTP and the httpd daemon, userids are assigned in a control file, not necessarily by verifying a password. Daemon programs often have privileges in RACF or in USS that let them assume the identity of other users. SQL injection is sometimes a serious risk because it is not addressed in the rush to get a working system out the door. All of these risks are easily treatable using well-known techniques. If you are a RACF administrator who grew up with mainfarmes, you may not be familiar the risks and protections. If so, take these two immediate steps: 1) issue the TSO command NETSTAT to learn what TCP/IP connections and programs are active and 2) Invite your telecomm guru to lunch, asking him to describe what each of those programs are, and which of the IP addresses are outside your organization. Over dessert, ask his advice on how to learn about TCP/IP secuirty and how to evaluate your mainframe TCP/IP. 3) Learn about the SERVAUTH resource class in RACF, describe it you your telecomm guru, and ask his opinion whether there is a need for it in your shop. You will find that mainframe TCP/IP is the most securable Internet platform in the world, if you and the telecomm guru implement the available tools sensibly.

- **LDAP (Lightweight Directory Access Protocol)** is a set of rules for communicating with a database containing information about users (similar to the RACF database). LDAP can be used to log a user onto a system (Its user records can contain a password, or it can call RACF.) Almost any computer platform including Windows, UNIX and z/OS can support an LDAP server. This is the program you talk to to log on. LDAP servers can talk to each other, and can establish trusts with each other, so if you log onto one of them, you're considered already logged on by the others. On Windows, Active Directory is an LDAP database. On z/OS, IBM gives us an LDAP server for free with MVS. It can talk to RACF, do RACF administration, sign users on (either by calling RACF or by its own passwords), and log changes to the RACF database. The new feature from IBM called Identty Propagation provides translation between RACF userids and LDAP names. (Please see the briefing on page 2 of this issue.)

- **Enterprise Extender** is a product from IBM that lets you connect your network to a business partner's network. You might use this if you are a bank and want to connect your mainframe network to the network of your credit card processor. Enterprise Extender uses the UDP (similar to TCP, but different in important ways) protocol to make this connection. Inside each UDP packet is an SNA message sent between the two networks. (SNA is ISystem Network Architecture, IBM's original protocol for VTAM networks.) Because each SNA message is enveloped in a UDP packet, some people believe that UDP firewalls and encryption provide protection. This misses a significant risk of network attacks based on SNA. Because such attacks are enveloped in UDP, they are not protect against by UDP proteciton. To learn whether you use Enterprise Extender, ask your VTAM system programmer. If you do use it, ask him who the business partners are, and what other business partners they are connected to. To learn more about risks and protections, see www.stuhenderson.com/appnsec1.pdf and www.stuhenderson.com/Enterprise_Extender_Security.pdf .

- **Blade Servers** (described in the last issue). These come with administrative software called URM (Unified Resource Manager). To learn more, see the Redbook IBM zEnterprise 114 Technical Guide http://www.redbooks.ibm.com/abstracts/sg247954.html?Open.

More Things to Protect:

Here are some recently added resources and concepts you will want to be familiar with, including with a description of what they do and the resource classes they use in RACF. Who in your shop do you think should be responsible for deciding whether or not to activate them?

- ***Context in MQ*** is information provided in the header of a message, possibly including time, date, userd, the platform the message came from, and accounting information..

- ***Topics in MQ*** (MQ allows you to define topics, and then to publish information about a given topic. Users can subscribe to a topic, when lets them automaticallyr receive all postings which are published on the topic. Topics are

organized in an up-side-down tree, simliar to the RACF group tree and to the directory tree on your hard drive. You control who can publish and who can subscribe to a given topic by using the resource class **MXTOPIC** (and **GMXTOPIC**) with rules of the form: **hlq.SUBSCRIBE.topicname** and **hlq.PUBLISH.topicname**

- ***Routines in DB2*** A routine is a user defined function or a stored procedure. (Both functions and stored procedures can be written in SQL or in standard programming languages like C. A function is invoked in SQL. A stored procedured is called using the SQL verb CALL.. Use RACF resource class **MDSNUF** to control user defined functions. Use RACF resource class **MDSNSP** to control stored procedures.

- ***Schemas in DB2*** are ways to group similar resources (such as tables, functions and stored procedures) together. Suppose you have a table named TAXINFO and you discover that you want to have a separate TAXINFO table for each of your three sales divisions: EAST, WEST, and CENTRAL. You would define each of these three names as a schema, and use the schema names as a prefix for each of the tables: EAST.TAXINFO, WEST.TAXINFO, and CENTRAL.TAXINFO. You might have related functions and stored procedures that you want to organize by sales regions too. You would include the schema name as part of the names of these resources as well. In RACF you control use of the schema names with the resource class **MDSNSC**.

- ***Dubbing of processes in USS*** is taking an MVS address space and making USS aware of it by creating USS control blocks such as the User Security Packet (which contains the UID of the user and the GIDs of its groups). This makes the address space a UNIX process. Until an address space is dubbed, it cannot talk to USS and USS can't talk to it.

What to Do About BPX.UNIQUE.USER? (Must Do If Using BPX.DEFAULT.USER)

Many of us use a FACILITY class rule named **BPX.DEFAULT.USER** which provides a default USS identity (UID and GID) for RACF userids that don't have an OMVS segment. This makes it easier for us when we suddenly have to let hundreds of users who don't have OMVS segments access FTP for example.

IBM plans to stop supporting **BPX.DEFAULT.USER** after RACF Release 1.13. They urge us to use instead a new FACILITY class rule named **BPX.UNIQUE.USER**, which has been available since RACF 1.11. This automatically generates an OMVS segment with a unique UID for any user who needs one.

BPX.UNIQUE.USER requires that your RACF database has been re-structured to AIM Level 3 (ask your system programmer). If you are not at AIM 3, ask your sysprog to put it on his to-do list, since you will want it for this, and for other features.

One advantage of BPX.UNIQUE.USER is that it assigns each user a distinct UID, where BPX.DEFAULT.USER assigned all its users the same UID and the same GID..

When a user without an OMVS segment comes into USS, if the BPX.UNIQUE.USER profile exists, then the BPX.DEFAULT.USER profile is

ignored. You will need to plan carefully for this, including address file access permissions for the default UIDs and GIDs. The RACF System Administrators Guide for release 1.13 gives good suggestions for how to approach this. If you use BPX.DEFAULT.USER now, you will want to plan ahead for this change.

Interesting Products

While we generally do not recommend or overly criticize software products, we think you will find the following new products of interest:

- ***DataSniff from Xbridge*** is a tool to find sensitve dataon your mainframe, so you know what you need to protect. Protecting sensitive data is easy once you know where it is. Finding it is the hard part. DataSniff from Xbridge has just the tool you need to locate sensitive data throughout your z/OS system.. For more info: Xbridge Systems, Inc., Theresa T. Tama, Regional Sales Manager, (703) 447-1391, theresa@xbridgesystems.com

NYRUG (New York RACF Users Group) and Tampa, FL RUG November 1, 2011 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 exact agenda is not certain at press time, so you might want to check the same site for exact details as they become final.

The Spring, 2012 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

Planned speakers (subject to change and in no particular order) include:

- Laurie Ward of IBM on **"RRSF with TCP/IP"**
- Simon Dodge on **"Identity Propagation"**
- Dave Hilliard of IBM on "**So, you LOST your <MASTER> keys?**" (INFO about ICSF, setting keys, planning for hardware and software changes (and HOW to handle IF those keys are really 'lost', new cards, a replacement card, whole new frames (say a z/10 to a z/196))
- Open Discussion on **Your Favorite Health Checker Checks**
- Hayim Sokolsky on "**RACF Rewind: Advanced Features**"

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. 5-8, 2011 in Bethesda, MD
Feb. 28-Mar. 2, 2012 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($2050)**
May 21-24, 2012 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
April 23, 2012 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** (**$2100**)
Nov. 7-10, 2011 in Clearwater, FL
May 1-4, 2012 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)
April 11-13, 2012 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 ..
- 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