RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 80):

This Issue's Themes:

- Sensible Encryption
- Sensible Password Rules
- Whose Job Is It?

Free Whitepaper Explains DB2 Security, Including the New Features

Download it for free by clicking on

www.stuhenderson.com/NewDB2.pdf

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

New Format for NYRUG and Tampa Bay RUG

Our meetings will now include a Five Minute Madness, a tutorial, and other innovations. Please see details inside this newsletter.

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, March 27, 2012 from 10AM to around 4PM.

PLEASE NOTE NEW FORMAT described inside this issue.

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 Fall date to be determined in 2012**)

Vanguard Conference in Las Vegas in 2012

It's scheduled for June 25-28, 2012 in Las Vegas, NV.. For details, go to: http://www.bestsystemzsecuritytraining.com/index.php

RUG Members Discount

Vanguard Integrity Professionals is offering an exclusive discount of $300 off Vanguard Security & Compliance 2012 conference registration fees to all RUG members. To claim this discount, please register and provide discount code **VSCRUG01**. at the time of registration.

Today's Quotation

"***The focus of an IS audit should not be whether IT is right or wrong; rather, the focus should be on whether controls are adequate to support some goal (such as supporting the financial audit control objectives).***"

Basic Backgrounder on Encryption and Digital Certificates

Here's a little bit of structured thinking to simplify these subjects. You probably know already that there are two types of encryption: synchronous (uses the same key to encrypt and to decrypt) and asynchronous (uses different keys to encrypt and to decrypt, the two keys being mathematically related to each other)

When to use each: Use synchronous encryption when you control both ends of the link, for example a link between your New York data center and your Los Angeles data center. You will insert the same key into the hardware or software at each end. The hardware might be a modem or firewall. The software might be RACF or a Kerberos server. Examples of synchronous encryption include DES and AES.

Use asynchronous encryption when you control only one end of the link, for example over the Internet. Asynchronous encryption is sometimes called "two-key" or "public key" encryption. Each pair of keys consists of a public key and a private key. If you encrypt with either one, you can only decrypt with the other. For this to work, you need a reliable way of telling a stranger over the Internet what your public key is. (You of course keep your private key secret.)

That reliable way is a digital certificate. A digital certificate is a message that tells you someone's public key. It should often be stored in the RACF database.

To determine how many pairs of keys (how many digital certificates) you need, ask yourself if the purpose is just to set up encryption, or something else (like client authentication or non-repudiation). If all you want to do is encrypt, then you need only one pair of keys, and that means one digital certificate. (You may need additional certificates to validate this one certificate, but the point is: you don't need a pair of keys for each user or each platform.)

Some questions: Who in your shop has the authority to decide what to encrypt? Who knows what needs to be encrypted and what laws apply? Who is responsible for making sure that what needs to be encrypted, is encrypted? To paraphrase the wisdom of Russ Hardgrove: "the RACF administrator: GUILTY until proven innocent."

What We Can Learn From the Wikileaks Story — Access Creep

While there is a lot of attention on "who leaked what", a more interesting question is "How were they able to do it?", along with "Who was responsible for preventing it?". Apparently the leaks were made possible by a US government internal, highly secure network. Access to the network was limited to a small number of people. Over time, more people (lots more) were authorized to access it, and more types of data were exposed on it. And no controls were put in place so that someone authorized to one type of data on the network couldn't access other data on the network. Access to the network meant access to all the data on it. People assumed that everything was OK, since "it's a secure network".

You've heard of "scope creep" on a project gradually making the project so big that its original purpose can't be achieved. This network appears to be a case of "access creep", with additional accesses gradually being added to the point that the original purpose of the "secure" network was lost. And no one was responsible for looking at the big picture and asking "Is this acceptable security?"

Thank goodness we don't have access creep in any RACF shops.

How to Recognize a Control Structure

Imagine that you're an end user, perhaps the head of Marketing. Someone from IS tells you that the new online marketing programs will work perfectly, making customers happy and increasing revenues. This makes you feel good, but you'd like to have better evidence than just the word of someone you don't know.

Imagine that you're an IS auditor and trying to find out if security is good enough to make the financial auditors happy. (The financial auditors are trying to answer questions like" "Can we rely on these numbers?", "Are assets protected?", and "Are we in compliance with all applicable rules and regulations?".) Someone in IS tells you that security works perfectly and can be relied upon. This makes you feel good, but you'd like to have better evidence than just the word of someone you don't know.

As an IS auditor, you can take one of two approaches. The first is to get a checklist of what someone thinks should be in place and see if what the data center has matches what's on the checklist. This has obvious shortcomings.

A better approach would be to look for a control structure, one which you can test intelligently to see, and to document, how good security is. A control structure will likely include:

- Formal policy assigning responsibility and authority for information security
- Formal standards and procedures for how security is to be implemented and maintained
- A meaningful assessment of risk
- A meaningful list of controls that are capable of being tested, and which, taken together, provide reasonable protection against the identified risk. These controls should be structured so that they can be broken into component pieces. For example, high level controls might include:
  - Operating system security can be relied upon
  - No one can use the system without being reliably identifed and authorized.
  - No one can access data without being authorized by (whoever the policy says is responsible for approving access)

The control "No one can use the system without being reliably identified" can be broken down into components such as:

a. Every path into the system is controlled by RACF.
b. No one can get a RACF userid without the approval of (whoever the policy says)
c. RACF userid and password administration function effectively
d. RACF options for userids and passwords make it difficult for someone to spoof someone else's identity
e. ... and so on

This will lead to a set of things that can be tested. The results of the testing can be rolled up to a conclusion, and the entire logic documented. This control structure, and the testing performed against it, can provide better assurance than just taking the word of someone you don't know.

You can use this concept to guide your auditors, providing them with lots of control structure information, and asking them to relate any checklists they use to actual risks, identified controls, and your policy, standards, and practice.

Password Hard Info:

With all the opinions about password length and encryption techniques (and attempts by people to remember junior high school probability theory), it's useful to have some firm facts to work with. Here's one real example of how long it would take for a password cracker program to figure out one password with passwords of different lengths. You do not need to memorize these numbers, but you might want to note the effect of adding just one to the password length.. Please note the difference in units (seconds, minutes, so on)

If RACF Password length is —>>	4	5	6	7	8
then CPU Time to crack is —>>	1 second	24 seconds	16 minutes	10 hours	17 days

This assumes that passwords are all alphanumeric (39 possibles for each character). Times have been rounded, and are based on the same CPU rating. Times are the CPU time to try every possible combination; so average times might be one half the values listed above. Times may be reduced if various optimization features are activated, or if a faster CPU is used. Numbers are provided courtesy of Peter Goldis' web site. You can try out his timings using different password rules and CPU ratings at www.goldisconsulting.com/predict.htm (He also provides us with with useful information on important issues and commonest methods for breaking into MVS. See www.goldisconsulting.com . Thanks Pete.

Some Important Password Points

1. Password length really does affect the difficulty of cracking.

2. If you have READ access to a copy of the RACF database, you can learn users' passwords with a cracker program.

3. Cracker programs do NOT add one to the count of invalid passwords for a userid, so userids don't get revoked.

4. Life is simpler if no one has READ access to the RACF database, especially if your SETR says "three strikes and you're out"

5. Life is even simpler if every started task userid is PROTECTED in RACF. The same applies for every other type of userid which is automatically signed on without a password, such as production batch userids.

6. Life is even simpler if users are trained to make passwords ***"easy to remember but difficult to guess***".

Advice from Google

(From a Google print ad in the New Yorker magazine) "***It's a good idea to have a different password for each of your important accounts,... but we know it can be hard to keep track of them all.***

So try thinking of a phrase that only you know, and that relates to that particular [account] to help you remember. For your email you could start with "My friend Tom sends me a funny email once a day" and then use numbers and letters to recreate it. **MfTsmafe1ad** ***is a password with lots of variations.***

Making passwords that are personal to you, and are different for each of your important accounts, will help keep you safe online. Which is good to know."

Getting Rid of Ghosts

It's almost a cliche on the RACF list server. Someone posts asking for help because some dataset or resource rules aren't working as they should. The next several posts are all some version of "Did you forget to turn on generics?" (because if you don't, then wildcard characters like asterisk and percent sign aren't treated as wildcards). Fans of Emily Litella recognize the original poster's response, "Never mind (but thank you)". (If you don't know her, you can Google her.)

You could almost say that you aren't a real RACF administrator if you haven't made this mistake at least once, or know someone else who did. IBM has now given us an improved method of dealing with such "***ghosts***" (non-generic rules whose names contain asterisks or percent signs.)

In release 12 of RACF for z/OS, IBM gives us the **UNUSABLE** flag in the RLIST and SEARCH output. This tells us that the listed rule contains wildcard characters in its name, but is not a generic rule.

IBM also gives use the **NOGENERIC** operand on the RDELETE command. This tells the command to delete the rule only if it is not a generic rule. This makes it easier to delete your ghosts.

You get the feeling that RACF has the reached the mature stage in life where the improvements in each release are careful refinements, that no significant shortcomings remain to be addressed.

Remember though: You want to leave SETR NOGENERIC for the digital certificate and keyring resource classes. They may need to use a percent sign as a percent sign.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
March 27, 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 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 Fall, 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

New Format for NYRUG and Tampa Bay RUG Meetings

Starting at 10am on March 27, 2012, 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, discussion of RACF requirements to pass onto IBM, RUG meeting logistics, 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 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**)
Feb. 28-Mar. 2, 2012 in Clearwater, FL
Dec. 3-6, 2012 in Bethesda, MD

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 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**)
May 1-4, 2012 in Raleigh, NC
Nov. 12-15, 2012 in Clearwater, FL

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.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.

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