RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 72):

Share Your APPN Security Stories with IBM We have an opportunity to pass along to IBM any concerns or incidents you care to relate regarding APPN security. If you want to take part, please email Stu at stu@stuhenderson.com. He will pass your email address or phone number to interested parties in IBM, who may or may not contact you to hear what you have to say. Have you had a better offer this year?

Wouldn't It Be Nice If There Were a Better Reporting Tool for Digital Certificates? There is, starting with the RACF Database Unload Utility output. There is shareware software available to produce reports from this output regarding digital certificates. See for example Nigel Pentlands' free offerings at

http://www.racf.co.uk/racf.pdf

on page 52. Reports 119 and 120 should be useful to you. [Hats off to Nigel and all the others who make our lives easier by sharing their good stuff]

Also, several of the third part software products such as IBM's zSecure and Vanguard's VRA provide such reporting.

How to Secure Mainframe FTP is described in an article at http://zjournal.tcipubs.com/issues/zJ.Dec-Jan08.pdf in the current issue of zJournal.

NEW YORK RUG Meeting Dates

Tuesday, February 12, 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 April, 2008. 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 a date to be announced 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.

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**

Password Rules and Auditors

Occasionally, an auditor will take a single point such as “Mixed case passwords are not used. You should require them.” and turn that into the entire audit finding/recommendation. This misses two important issues, which are worth raising:

1) Is there some standard that says whether mixed case passwords are required, either a law/regulation or a company standard? If not, then the auditor is just expressing his opinion. It should be treated as that, just one person’s opinion, unless the auditor demonstrates why this is important (which leads us to the second issue:)

2) What is the control objective, that is the purpose of even looking at the use of mixed case passwords? If the auditor cannot relate the finding to a reasonable control objective, then the auditor has likely failed to show the relevance of the finding. Suppose however that the auditor has stated as a control objective: “Ensure that no unauthorized user can access the computer system.” Then, the comment on use of mixed case passwords is just one component of the evaluation of controls. The auditor should also be considering several other findings, such as:

1. What is the minimum password length, and what characters are allowed?

2. How many invalid passwords does it take to revoke a userid?

3. Are the PROTECTED and RESTRICTED user attributes used?

4. Are all paths into the system controlled by RACF (including NJE, RJE, batch jobs, FTP, USS, and every applid)? If a program (applid) has its own hard-coded list of userids and passwords, then for that path into the system, the use of mixed-case passwords in RACF is irrelevant.)

5. Who has read access to ANY copy of the RACF database? (Including tapes, copies sent off site, full pack dumps of disk packs, users with the OPERATIONS attribute, started tasks marked TRUSTED, and others) Anyone who can read the RACF database or its backup could run a password cracker program against it and learn everyone’s password. By requiring mixed case passwords, you might make it harder to guess a password, but if it takes 10 hours instead of 3 hours for the cracker program to run, this may not be important.

6. Does the Help Desk reliably verify a caller’s identity before resetting a password?

7. Are user’s well-trained in how to make passwords “easy to remember, but difficult to guess”?

8. Are pass phrases used? (Or will they be used, once software such as TSO and CICS are able to support them?)

9. What are settings for other password rules, such as password interval, password history, and automatic revoke after x days of inactivity?

All of these points (and several others we don’t have room for) contribute to any conclusion as to how well an installation prevents unauthorized users from accessing the system. Auditing is defined as “evaluation of the adequacy of controls to achieve some purpose”. A control is defined as the “comparison to a standard to achieve some

purpose". So if an auditor addresses all these points (each of which can be a comparison to a standard), in order to evaluate how well a specific control objective is achieved, then the auditor is adding value. If an auditor just takes one of these points out of context, and doesn't relate it to a specific objective, then the audit will be less useful.

Unless your installation is clearly in violation of some law/regulation/company policy, an auditor's recommendation can be stated as a practical suggestion, for example:

> *In the light of all the (previously described) controls and the importance of the data on this system, the risk of someone guessing someone else's password seems higher than necessary. To reduce this risk, you should consider tightening the controls (for example by requiring mixed case passwords and by reducing the password interval from 150 to 30 days)*.

As RACF administrators and Data Security Officers, we have a responsibility to help our auditors to do the best job they can. Discussing issues such as these at the start of the audit in particular can help them to understand our expectations of their performance.

Resource Class Rules of Thumb and Exceptions

Four Rules of Thumb for RACF resource classes can help simplify administration, as long as you pay attention to the exceptions. (Readers are invited to add to this list, either useful rules of thumb or additional exceptions.):

- You can solve the "protectall issue" (what happens if no matching rule) by defining a "backstop" rule, that is a rule named **, for a resource class. Make the **UACC** be **NONE** or **ALTER**, depending upon your taste. Make the rule say "**AUDIT(ALL)**" to learn of every RACF call using the rule. **DO NOT MAKE SUCH A RULE FOR THE FACILITY CLASS**, and perhaps not for certain other classes. This is because some decisions are based on whether a matching rule exists, not on what it's UACC is. Do not make the name of the rule be * (a single asterisk), since that would make it difficult to list just that one rule with

  RL classname * ALL

- You can be sure that you learn of any changes to resource rules if you turn on audit for a class [**SETR AUDIT(classname)**], which can be viewed in the Class Descriptor Table in DSMON. This causes logging to SMF of any change to a rule in the class (Creation and deletion are just extreme forms of change.) However, do not use this with the USS classes named: **FSOBJ**, **IPCOBJ**, and **PROCESS**, since with these classes AUDIT has the effect of generating SMF data when objects are accessed as well. A possible approach would be to issue:

  SETR AUDIT(*)
  SETR NOAUDIT(FSOBJ IPCOBJ PROCESS)

- It can be beneficial to turn on generics for a resource class **[SETR GENERIC(classname)]** so that asterisks and percent signs get treated as wild cards (and not as asterisks and percent signs). This can protect you from the

embarrassment of creating resource rules, wondering why they don't work, and then discovering that they contain asterisks which are not treated as wildcards.

EXCEPTIONS: IBM recommends strongly that you not turn on generics for resource classes relating to digital certificates, since these rules may have names which include real asterisks and percent signs which you don't want to have treated as wildcards. You might want to issue:

SETR GENERIC(*)
SETR NOGENERIC(DIGTRING DIGTCERT)

Another approach would be to make sure that any time you create a new resource rule with a wild card in its name, you verify that generics is active for the class. Or be sure to list the rule and make sure that it's name appears with a **(G)** after it to prove that it is a generic rule.

- Have a clear decision for each resource class on whether to use it in your shop or not. Have someone knowledgeable who is responsible for deciding whether to use the class or not. (Think of **VTAMAPPL**. Is it ACTIVE in your shop? Who is responsible for the decision? If no one is clearly responsible, then the default is that the RACF administrator is responsible, since "You're in charge of security, aren't you?")

  EXCEPTIONS: The **PROGRAM** and **GLOBAL** resource classes are not activated with **SETR(classname) ACTIVE**. Instead, **SETR WHEN(PROGRAM)** and **SETR GLOBAL(otherclassname)** are used.

What Are Digital Certificates and PKI and Why Should I Care?

A digital certificate is a message that tells you someone's public key. (With two-key encryption, keys come in matched pairs: one is private and the other is public. You encrypt with one key and decrypt with the other. Or you can encrypt with the other and decrypt with the first key. In either case, you need a reliable way of knowing someone else's public key. This is the role of the digital certificate.)

PKI or Public Key Infrastructure is the set of policies, procedures, and standards for administering public keys and digital certificates. This includes for example making sure that certificates are reset before they expire and that they provide a reliable way of supporting encryption over the Internet when needed.

Help, I've Inherited Someone Else's RACF Database with NO Documentation of All the Digital Certificates and What They're For!! What Do I Do? (Corrected version with warm thanks to Wai Choi for excellent suggestions)

Our simplified approach has three phases: weeding out, sorting, and analyzing. Start by listing all the digital certificates and keyrings, with commands like:

RLIST DIGTCERT * ALL
RACDCERT LIST CERTAUTH
RACDCERT LIST SITE
RACDCERT LIST ID(one userid)

You might also use the SEARCH command to get the names of all the profiles in

the DIGTCERT, DIGTRING, DIGTNMAP, and DIGTCRIT classes. Note that the RLIST command gives information (OWNER and APPLDATA) not listed in the RACDCERT command, and that RACDERT LIST ID(..) can only list one userid at a time (no asterisk permitted). Third party software or freeware can help with this (please see page 1.).

1) **Weeding Out** You can ignore every digital certificate marked NOTRUST, since these have no effect. You can also ignore any certificate whose expiration is past, since it should also have no effect.

2) **Sorting** Organize the remaining certificates into three groups, based upon their types (**CERTAUTH**, **SITE**, or **USER**).

A CERTAUTH or certificate authority certificate is one that is signed by the private key of a well-known, trusted certificate authority (such as VERISIGN). IBM puts these CERTAUTH certificates in the RACF database automatically, but marks them all initially NOTRUST. You can use the RACDCERT command to mark them TRUST. The public keys corresponding to the private keys for these certificates are already, automatically installed in Internet Explorer (or whatever your browser is).

A SITE certificate is one that represents a server in your network or that is used to share a single certificate and its private key over several RACF userids. It can be used to sign other certificates.

A USER certificate is associated with a specific RACF userid. The **APPLDATA** field of the resource rule will list the userid the certificate is associated with. All his keyrings will have names whose first part is the userid itself.

3) **Analyzing** Now you're ready to see the relationships among the certificates. There are two types of relationship: keyrings and certificate trails.

A keyring is a collection of digital certificates associated with one userid. (They may be owned by different userids, but are used to provide one userid's public key.) The name of each keyring is sometimes listed with that userid and a slash (/). So list the keyrings one-at-a-time. For each one, verify that the information in the user record, the keyring, and the certificates all match.

For certificate trails, you want to review which certificates are used to validate which other certificates. Each user certificate will be signed by another certificate (which may be signed by another certificate, and so on), back to a CERTAUTH or SITE certificate. The CERTAUTH or SITE certificate will be signed with a private key whose public key must be installed in Internet Explorer (or whatever your browser is). (If it isn't already there, you'll have to get it installed.) This makes it possible for your browser to validate the certificates, starting with the CERTAUTH or SITE certificate whose public key the browser knows. Your browser relies on the public key in the CERTAUTH or SITE certificate to validate the next certificate in the chain, whose public key will allow the browser to validate the next certificate in the chain, and so on.

In each certificate, check the **Issuer's Name,** the name of the certificate that validates the certificate you are looking at. Look also at the **Subject's Name,** the name of the certificate itself. Map these two fields in the certificates, to

determine which certificate is to be used to sign or validate which other certificates. Then verify that this validation holds up.

So for each userid, you will want to see what certificates are in its keyring or are otherwise associated with it. You will want to be sure that all these certificates are needed, and that they form a reliable chain to let your browser validate the USER certificate. Once you've completed this analysis, you should be able to recognize the role that each certificate plays in your security.

Later you will want to address certificate name filters and virtual keyrings. We will save that for another time.

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 a date to be determined shortly.

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**)
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 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**)
May 5-9, 2008 in Raleigh, NC
Nov. 17-20, 2008 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.) ($1560)
May 20-22, 2008 in Bethesda, MD

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. Hayim will speak on JES security and on RACF/DB2 conversions
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: **February 12, 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/Feb12RUG.doc

.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