RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 77):

This Issue's Themes:

- Control Every Path Into the System, Ford Every Stream,

Another Great Source of Free, Practical Info:

Mark Nelson of IBM has updated the 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

The Password Fallacy:

Some people choose to spend time discussing such things as whether the minimum password length should be six or seven or eight. To put this into perspective, it helps to remember that the whole purpose behind this is to prevent users or hackers from being able to guess others' passwords.

Assume that a userid gets revoked anytime there are three bad passwords in a row. Assume we require alphanumeric, which in RACF means at least one number and at least one letter, but we don't specify where.

How much does it matter then whether the minimum password length is six or seven? Not much at all. And even better if you say the length must be from six to eight. Think about it. Do the math.

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, October 26, 2010 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,

---

NY Metro NaSPA Chapter (system programmers professional association) meets Oct. 19 The NY Metro NaSPA Chapter meeting will be on 19 October at IBM, 590 Madison Avenue, room 1219, from 10AM to 4PM. We'll be focusing on the latest announcements from IBM: the new z/196 processor and z/OS V1R12. You are warmly invited. Please RSVP to Mark Nelson at markan@us.ibm.com

The meeting is open to non-NaSPA members and is free! Please pass this invitation on to your colleagues!

Today's Quotation

"*When you think about it, of all the things we do, taking care of each other is the only thing that matters.*"

The Biggest Security Hole in Your Mainframe: may be Windows. Here's why: Users log onto the mainframe from Windows computers which are part of a Windows LAN (Local Area Network). If Windows is not configured to use Kerberos, then they run the risk of someone installing a sniffer program to learn userids and passwords, including mainframe userids and passwords, as they go by. Implementing Kerberos (with Active Directory) on the LAN both improves security for everyone and reduces resource usage.

Yet More Great Sources of Free, Practical Info These are from IBM's Gwen Dente:

- Link for the IBM Academic Initiative Program (listings of universities offering courses, etc.): https://www.ibm.com /developerworks/university/academicinitiative/

- Link for z/OS Skills Basic Information http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp

Webcast: z/OS TCP / IP Networking Conference November 10, 2010:

Learn more about IPv6 Security, PKI, and Network Security for Dummies. For more info, please visit http://www.insidethestack.com/networkconference.html

Paths Into the System: Self-Assessment:

Last issue we gave you a self-assessment for your protection of data. This issue we show you how to conduct your own self-assessment of the paths into your system. Any path into your system which is not controlled by RACF represents a possible security exposure, since it can permit people into your system even if they are not defined to RACF.

Here are the paths into your system:

- **TSO**
- **Started Tasks**
- **Batch Jobs**
- **USS**
- **NJE/RJE**
- **TCP/IP and his daemons**
- **Other applids**

For each path we'll show you how to make sure tha RACF controls it completely. In some cases, you'll use switches like **BATCHALLRACF**. In other cases resource rules in the **APPL** or other resource classes. You need to walk down each path to make sure RACF controls it properly.

TSO:

When someone types a userid and password into TSO, TSO calls RACF. You can use the **APPL** resource to restrict who is allowed to come into TSO. (This is described in issue 75 of this newsletter.)

If you try to log onto TSO and RACF tells TSO "I don't have a user record for that userid.", thenTSO looks to see if the userid and password match an entry in the dataset **SYS1.UADS**. If so, then you get logged onto TSO with that entry from UADS, and RACF considers you an Undefined User. (Undefined users can read datasets with a UACC of READ. They can't read datasets with a UACC of NONE and a permission of ID(*) with READ.)

(Cont'd)

(Cont'd)

Started Tasks (aka Started Procedures):

When someone issues the **START** command to start a started task, RACF uses the **Started Procedures Table** to assign a userid to the started task. You can see both parts of this table in the DSMON report. The oldest part is named **ICHRIN03** and is an assembler language module. The newer part is made up of entries from the **STARTED** resource class. An entry of * matches every started task name, and ensures that every started task is assigned some RACF userid, giving RACF control of this path into the system.

Batch Jobs:

Batch jobs are required to have a RACF userid if the switch **BATCHALLRACF** is active. You can see this in **SETR LIST**, along with **XBMALLRACF**. (**XBMALLRAC**F is meaningless in most shops. It functions like **BATCHALLRACF**, but only applies if you are using the JES eXecution Batch Monitor. Ask your JES sysprog. If you aren't using it, then it should cause no problem to turn **XBMALLRACF** on.)

USS:

USS (UNIX System Services) is UNIX under the control of MVS and RACF. USS doesn't let you in unless your userid has a valid **OMVS segment** with a valid **UID**, and it must belong to at least one RACF group with a valid **OMVS** segment and valid **GID**. You can also use the **APPL** resource class, with a rule named **OMVSAPPL**, to control access to USS. Note that it is possible to assign a default UID and GID to RACF userids by means of a **FACILITY** class rule named **BPX.DEFAULTUSER.**

NJE / RJE:

NJE (Network Job Entry) and **RJE** (Remote Job Entry) are ways for remote sites to submit work to **JES** on your computer over telephone lines. The work can be batch jobs, operator commands, and printouts. You can control what batch jobs enter your system this way by means of **BATCHALLRACF** (described above under Batch Jobs). You can also use the **NODES** resource class to control assignment of userids and access to your system for both batch batch jobs and printouts. Use the **WRITER** resource class to control where the printouts can be routed. And you can user the **OPERCMDS** resource class to control who can issue operator commands on your system remotely. If you don't know already, ask your JES sysprog for the names and locations of all your NJE and RJE connections.

TCP/IP and his Daemons:

You control access to your system through **TCP/IP** by controlling **IP addresses** and **ports**. (An IP address corresponds roughly to one computer, and often to one **DNS** name such as www.yourcompany.com. A port corresponds to one application such as email or FTP on that one computer. So a TCP/IP message will be routed to the correct computer according to its IP address, and once at that computer to the correct application according to its port number.)

Each daemon (application program such as **FTP** or **email**) has its own control file which specifies how it identifies users to RACF. Daemons can include programs like **FTP**, but also **CICS**, **DB2**, **MQ Series**, and other MVS system software talking to the Internet. **Firewalls** can provide control over who can use which IP addresses and which ports, but if you're the RACF administrator, you probably don't have control over firewall rules. You can however use RACF to

force proper change control over the configuration files for TCP/IP and for each of its daemons.

You need to become familiar with each TCP/IP application and its control file. For example, the **FTP** control file can permit Internet-based submission of batch jobs, selection of DB2 tables, and browsing of printouts, all of which should be controlled by RACF.

Use the TSO command **NETSTAT** to learn what TCP/IP connections are active. Use the **SERVAUTH** resource class to control access to TCP/IP itself, and to control use of IP addresses and ports. Note the risk of someone executing a rogue program on the mainframe which opens a port and starts communicating over the Internet. You can prevent this by controlling who is allowed to open a port (by means of the TCP/IP configuration file and/or the **SERVAUTH** resource class.)

Other Applids:

Other applids include CICS, IMS, and addiitonal programs with sign-on screens such as OMEGAMON. You need a policy requiring each applid to invoke RACF to verify userids and passwords. (The alternative is hard-coded lists of userids and passwords, which can allow someone access to your system even after you have revoked his RACF userid.) Many applids (including CICS, IMS, and OMEGAMON) can use the **APPL** resource class with RACF to control who can sign onto them. You might for example want to let programmers into the test CICS region, but only end users into the production region.

At the end of this analysis, you should be able to say that every path into the system is controlled by RACF. You probably do not have adequate security until you reach this point. This is sort of like having **PROTECTALL** on for datasets, except it applies to system access.

A Security Surprise with USS:

_____You may think you understand UNIX security, so here's a way to test yourself: If a user has UID(0), that is, superuser privilege, can he then do anything to any UNIX (or USS) file?

The answer is YES, with one exception: if he wants to execute a program file and none of the permissions (user, group, or world) has the EXECUTE bit turned on, then he can't execute it, even though he is superuser.

_____Bruce Wells of IBM pointed out that there is a clear explanation of how this all works in Appendix E of the RACF Security Administrator's Guide. Apparently this is not a RACF quirk, but standard UNIX logic, which RACF graciously reflects. Thanks, Bruce.

Rules of Thumb for CICS Security:

To make life easier for the RACF administrator,

- Have a unique userid for each CICS region. Put them all into a group of "ALL CICS REGIONS" or 'ALL PROD. REGIONS' if you want to treat them the same.
- Have a unique default userid for each CICS region. Put them all into a group of 'ALL CICS DEFAULT USERIDS' if you need to treat them the same.
- In the program properties table, don't tell the system not to call RACF for CICS.
- Don't give CICS region userids, nor their default userids privileges such as OPERATIONS or SPECIAL
- When CICS is a started task, don't mark it TRUSTED nor PRIVILEGED
- When a new region gets created, add its userid in a PROPCNTL resource rule. This will prevent its transactions from submitting batch jobs that inherit the userid of the region. (It would be nice to do this with existing CICS regions, but may not be practical if lots of applicaitons already depend on this ability.)
- Ask the CICS system programmer to tell you of any CICS regions that use MQ series, or IMS, or DB2, or talk to the Internet. You will want to secure them properly up front.

Two CICS Tricks

The First One: A user once tried to issue a sensitive CICS command without logging on, and succeeded. This was after his terminal had a bind, but before he bothered to do a sign-on. Later research showed what had happened: the default userid for the CICS region was permtted to the transaction. Any user doing anything who hasn't signed on executes under the authority of the default userid.

A lesson learned is not to permit this userid to sensitive transactions. You might want a chart on your wall listing all the regions, their userids, their APPLIDs (for both the APPL and VTAMAPPL resource classes), and their default userids.

The Second One: When two CICS transactions execute at the same time in the same region, each one can read and alter the data belonging to the other, unless you prevent it. This is because each CICS region is a single address space (as is each batch job, and each TSO signon). All the transaction programs in the region execute by default with Protect Key 8. Being in the same address space, and having the same Protect Key, means that you can access each other's memory.

(Address spaces and Protect Keys are hardware controls that MVS uses to build a virtual cage around each address space, so programs in one address space can't touch the memory of programs in a different address space.)

This is not a problem if the region is used, say, only for Production Accounts Payable Transactions. In cases where for example, both Production Accounts Payable and Test Marketing transactions execute in the same region, this creates a risk.

(If you've ever worked as a CICS applications programmer and had someone else's buggy transaction program cause your program to fail, you'll know exactly why this is not desireable.)

Fortunately, CICS gives us an option in the **SIT** (System Initialization Table, where the system programmer specifies the options for the region) named **STGPROT**, which can reduce this risk.

NYRUG (New York RACF Users Group) and Tampa, FL RUG
October 26,, 2010 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 to Hayim Sokolsky (hsokolsky@dtcc.com) with "NYRUG" or "Tampa RUG" in the subject line and your name, company, phone, and email
You must register for the NYC meeting in advance (Click here if reading this online.)

Please note that speakers no longer provide copies of handouts. You can print your own copies from this link: www.stuhenderson.com/handouts.HTM . 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/NYRUG.HTM .

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 75 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.
You must register for the Tampa meeting in advance. (Click here if reading this online)

For complete directions, please go to: www.stuhenderson.com/NYCRUG1.pdf Or to: www.stuhenderson.com/TampaRUG1.pdf .

Speakers (subject to change) may include:

- " ***Vanguard Administrator - Little Known Features***" by Jeff Benson of Guardian Life
- "***What's new to help you better manage RACF***" by Jeffrey Johnson of IBM
- "***Custom Fields Forever***" by Hayim Sokolsky of DTCC
- Three New z/OS V1R12 Items:
  - o "***Ghost (invalid) generic support***" by Scott Woolley of IBM
  - o " ***New saftrace filters***" by Scott Woolley of IBM
  - o "***Enhanced generic loading (BIG performance Item)***" by Russ Hardgrove of IBM
- "***Clear Explanation of Digital Certificates***" by Stu Henderson
- "***How RACF Always Call Came To Be***" by Rich Guski, IBM Retired
- "***Is Your z/OS System Secure?***" by Ray Overby
- "***How to Manage IS Auditors with Checklists***" (time permitting) by Stu Henderson

Interesting Products:

ERQ [Easy RACF Query] provides comprehensive, yet simple, on-line RACF administration and reporting. Easily CLONE, DELETE, LIST and/or REPLICATE profiles with a single key stroke. ERQ offers a fully customizable ISPF interface for flexible and efficient RACF Administration, as well as easy to-use Programming Services for writing custom RACF application/procedures using a straightforward API interface. Users can easily issue commands or generate reports with little or no training.

For more info, contact: **Lisa Hamilton**: Phone - 239-649-1548 Ext. 210 or Email - Lisa.Hamilton@aspg.com

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. 6-9, 2010 in Bethesda, MD
   Mar. 1-4, 2011 in Clearwater, FL

2) HG05 **Advanced RACF Administration ($2050)**
   May 23-26, 2011 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
   April 11, 2011 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) HG62 **Comprehensive Information Systesm Auditing with Case Studies** (**$1200**)
   Nov. 4-5, 2010 in Bethesda, MD

B) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$2100**)
   Nov. 16-19, 2010 in Clearwater, FL (class is full. 2011 dates coming soon)

C) 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 6-8, 2011 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 ..
- 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 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