RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 97):

This Issue's Themes:

- New Stuff Coming, Learn a Little Bit Now
- Learn at home or office online - 4 ways

Free Webinars: NewEra sponsors great webinars each month :

See the schedule at:
www.newera-info.com/Month.html

If you miss these, you can get recordings and copies of handouts at
www.newera-info.com/Presenters.html

White Paper

How to Manage Encryption on Windows, UNIX, and Mainframes
A Simple Guide for CIOs, CISOs, Security Admins, and Auditors

http://www.stuhenderson.com/EncryptionMgt.pdf

Where to get info on new stuff
(From the RUG handouts page, for the RUG meetings)

http://www.nyrug.stuhenderson.com/handouts.HTM

NEW YORK RUG Meeting Now Online and Open to Everyone: May 12, 2020 from 10AM to near 4PM *NYC time..*

THIS IS A LOT OF TRAINING AVAILABLE IN ONE DAY. **You will not be allowed to take part without pre-registering (it's free).** To pre-register, please visit
www.nyrug.stuhenderson.com
See inside for details. (The meeting after that will be **in the Fall of 2020**)

If you want reminders of upcoming RUG meetings, please click RUG Reminders to receive one email reminder before each meeting (two per year).

Please Note the New Website for the NYRUG and TBRUG and Raleigh and Dallas RUGs: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG and Raleigh and Dallas RUGs at
www.nyrug.stuhenderson.com

Today's Quotation

"*The only way to find where a limit is, is to cross it.*" ---Anonymous

---

Henderson Group RACF and Audit Seminars Now Offered Online

For details, please go to:
http://www.stuhenderson.com/VirtualSems.html

To subscribe to this newsletter, or for back issues:

http://www.stuhenderson.com/Newsletters-Archive.html

RACF Bypass in Tape Management Software

A colleague discovered that he could read some tape datasets, even though RACF quite properly denied the access request. After some research it was learned that the tape management software (in this case IBM's DFSMSrmm) has options that can bypass RACF, allowing access even when RACF says not to.

These options are set in the configuration file for DFSMSrmm. The RACF administrator had not been aware of this. We might all want to pay more attention to protection of tape datasets, including tape management software settings, Bypass Label Processing, the 17 character dsname problem, and the two datasets on a cartridge problem. You can learn more at http://www.stuhenderson.com/TAPESEC1.PDF .

The Least You Need to Know About LDAP

If you are a RACF administrator, LDAP may be coming at you rapidly. Here's the minimum you need to know about it.

Imagine you are a UNIX user logged onto a UNIX computer. You want to log onto some other UNIX computer. But your userid isn't defined on that computer. You wish that you could tell the other computer to trust your user definition on your computer. That's what LDAP does.

With LDAP, the software on each computer that checks out who you are (such as userid and password) can be told to trust the software and user definition on some other computer. So if my userid is defined on COMPUTERA and I want to log onto COMPUTERB, I can. At least I can if COMPUTERB's LDAP software is set up to trust the LDAP software and user definitions on COMPUTERA.

Wouldn't It Be Great If We Could Expand This to Windows Computers Too?
Yes, which is why Microsoft has made the Active Directory Database an LDAP database. Windows supports LDAP with Active Directory.

Wouldn't It Be Great If We Could Expand This to z/OS on the Mainframe?
Yes, which is why IBM gives us LDAP for free as part of z/OS. LDAP on z/OS works with LDAP on UNIX and Windows.

Wouldn't It Be Great if LDAP on Mainframes Worked with RACF?
Yes, which is why IBM has made this happen. For details, see the handouts from the May 12 RACF User Group Meeting. Handouts can be found at http://www.nyrug.stuhenderson.com/handouts.HTM when available.

What Does LDAP Stand For?
LDAP is for **Lightweight Directory Access Protocol**. Protocol just means a set of rules. A directory is a (mostly read-only) database of user definitions, sort of like a telephone directory, aka phone book. LDAP is lightweight because it is a stripped down version of an earlier protocol you probably don't want to learn about.

Does LDAP Rely on USS (aka OMVS) and mainframe TCP/IP?
Yes, which makes sense given that LDAP was first developed on UNIX.

Why Do I, a RACF Administrator Care About Mainframe LDAP?

Because LDAP on the mainframe relies on RACF for two important functions:

- Translating RACF userids to LDAP user names
- Establishing trust among LDAPs on differnent platforms

What Sort of Naming Conventions Does LDAP Have for Userids?

Each full username in LDAP has several parts, starting with, for example **C=US** (country is US) and **O=MyCompany** (for organization is MyCompany). You have seen these before if you've ever administered Active Directory on Windows. It is usually better to have a single set of naming standards for LDAP names in an organization, as opposed to having several different standards for different departments.

Where Else Have I Seen That Type of Name?

In digital certificates. Did we mention that it's a good idea to have a single set of standards for your whole organization's LDAP names? The naming structure lets you set up individual sub-areas or zones within C=US and O=MyCompany. For example, you could add to those (this is a hierarchical tree, isn't it?): OU=unixguys (for Organizational Unit is unixguys) and OU=windowsguys and OU=mainframers.

How Does LDAP Relate to Kerberos?

LDAP has to do with the storing of user definitions, the trust between different computers, and the hierarchical naming structure that organizes them all..

Kerberos is a related protocol used to perform the verification of users' identities (similar to RACF checking out your userid and password). Kerberos can also set up an encrypted tunnel between two computers. Windows with Active Directory supports Kerberos. So does z/OS.

I'm a Little Geeky; How Do I Learn More Details?

Try these sources for more info:

- Presentations and handouts from the May 12 RACF User Group meeting See http://www.nyrug.stuhenderson.com/handouts.HTM
- IBM manuals
- Cross-Platform Security Recommended Solutions for Common Problems
- How Kerberos Works with LDAP
- Cross-Platform Security Considerations

Why You Have to Consider SSL or Kerberos or Both (the 800 Pound Gorilla in the Room We All Try to Ignore)

Many installations have most of their online users sitting at personal computers instead of the old, hardwired terminals. Users log onto the LAN (Local Area Network) which connects the PCs together. Once logged onto the LAN, they log onto the mainframe through the LAN. Since the architecture of a LAN sends every message to every workstation on the LAN, each user's signon stream (mainframe userid and password) travels to every PC on the LAN (or at least on the sub-net, or up to the first switch or router).

This means that any computer on the LAN can see every userid and password as they go by. To see this, you need a type of program called a sniffer. Sniffer programs can be downloaded for free over the Internet. They execute on a personal computer and read every message that goes by on the LAN. You can even specify filters, so they only pay attention to messages that contain the words: login, userid, or password. This makes it easy to learn someone else's mainframe userid and password, if you can get access to the LAN cable. (Good thing the security guards in our lobby only allow honest people into our building.)

If you don't believe this, you can try it out. (But don't do this without getting your manager to approve the experiment first. Many people get upset when you demonstrate that there is a gorilla in the room.) Get a laptop and download a sniffer over the Internet. Walk into your manager's office, pull the ethernet cable out of his desktop computer, and plug it into your laptop. Start the sniffer running on the laptop and see the messages from other workstations as they go by. Disconnect as soon as you have proved the point, and before you see anything compromising.

Encrypting your userid and password won't protect against sniffers, since all they have to do is record the encrypted message and play it back without decrypting it.

Two approaches will protect against sniffers: Kerberos and TLS (Transport Layer Security, which has replaced SSL (Secure Sockets Layer). Not all programs such as TSO and CICS support both of these thoroughly yet, but RACF and TCP/IP do. Deciding which one is best in your organization and getting people to work together to implement it would be a good way to fight boredom.

What Are Secure Containers?

IBM has bought RedHat LINUX. IBM's business strategy includes the market for "hybrid clouds". Imagine that your CIO has put some of your applications on a Microsoft Azure cloud. And other applications on an Amazon AWS cloud. And because some applications are so important that you don't want to trust them to some other organization where you have no idea what the security and reliability are like, some applications stay home on a mainframe cloud. (Yes, IBM supports your own in-house cloud on the mainframe.) To put this altogether, you want a hybrid cloud.

Well, suppose you want an application on one cloud to communicate with another application on a different cloud. Or you want to move an application from one cloud to another? The way to do that is called "**secured containers**". This is a set of rules to let you do that securely. To learn more, see the handouts and presentation from the RACF User Group Meeting at
http://www.nyrug.stuhenderson.com/handouts.HTM

RACF Survey: All questions optional

We'd like to make the RACF User Groups more useful to you. We hope you'll take a few minutes to tell us a little bit about what you would like from the RUGs, from the RACF User News, and from RACF. Feel free to answer as many of the questions below as you care to, and email to stu@stuhenderson.com. Thanks.

1. What RACF-specific topics would you like to hear more on?

2. What mainframe-not-RACF-specific topics would you like to hear more on?

3. What non-mainframe-but-still-security topics would you like to hear more on?

4. What other topics would you like to hear more on?

5. How important is it to you to be able to attend meetings in person?

6. Would you be interested in online meetings, such as via WebEx?

7. What else would you like to get from your RACF User Group?

8. What changes would you like in user group format, timing, logistics, location, other?

9. What else would you like from the RACF User News?

10. If you care to share something about your background, are you:

___ a RACF administrator

___ a system programmer

___ a consultant

___ a software vendor

___ an auditor

___ other? _____?

11. What else would you like, or what else would you like us to know?

National Association of System Programmers Meets Online April 22 10am to 3pm (more, free virtual training)

The next NY Metro NaSPA Chapter meeting is on Wednesday, 22 April, from 10:00 A.M. until approximately 3:00 P.M. For the first time ever, this will be a WebEx only event, starting at 10:00 A.M.

The three sessions below are on the agenda:

"Upgrade to z/OS V2R4 Part 1: Planning", Marna Walle, IBM
"Upgrade to z/OS V2R4 Part 2: Technical Actions", Marna Walle, IBM

"Virtual Storage Analysis: Exploring Below the Bar Private Storage Problems", Patty Little, IBM

Registration: No registration is required for this session!. However, I ask that you **RSVP to me (markan@us.ibm.com) in case there is a change to the WebEx information**.

WebEx Information:

Meeting link:
https://ibm.webex.com/ibm/j.php?MTID=m3b1a7bfd8cf9ba3b693e68926efdaea3

Meeting number: 494 962 282

Password: WebExOnlyNaSPA (93239665 from phones and video systems)

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

NYRUG Meeting is Online, Open to Everyone

May 12, 2020 from 10AM to 4PM:

Our next meeting is online, over the Internet only. Everyone is invited to take part, but you need to register in advance at www.nyrug.stuhenderson.com. While you're there, click on Handouts to get your own hard copy of the speakers' handouts.

The meeting after that will be in the Fall of 2020.

HG Effective RACF Administration Training and Mainframe Audit Training Seminars Now Offered Online

The Henderson Group offers its RACF and information security/audit seminars online, 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 RACF administration 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.

HG04 **Effective RACF Administration** (**$2195**)
November 9-12 , 2020 in Bethesda, MD

For mainframe audit training, please see: www.stuhenderson.com/XAUDTTXT.HTM.

HG64 **How to Audit z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)
November 16-19, 2020 in Bethesda, MD

Interesting Products We have not formally evaluated these products, but think you will find them interesting.

Many z/OS shops are not yet leveraging the SMF 119 zERT data to be able to prove (or identify and address issues) that all IP traffic is sufficiently encrypted. IntelliMagic offers a service to analyze the data for you:

Encryption Compliance Analysis

or to allow you to use the analysis solution yourself:

Monitor z/OS Network Traffic with IBM zERT

RACF User Services (Newsletter Subscriptions / Key Phone Numbers / Addresses)

Technical support hotline, Meetings, Seminar Catalogs:

Stu Henderson - (301) 229-7187, 5702 Newington Rd, Bethesda, MD 20816

stu@stuhenderson.com

For Back Issues of this Newsletter, Subscriptionsand Links to Several Useful Web Sites

check the Henderson Group website at: http://www.stuhenderson.com/Newsletters-Archive.html

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 see back issues or to subscribe to the Mainframe Audit News (MA News), check Stu's website at http://www.stuhenderson.com/Newsletters-Archive.html

To Get a Free Subscription to the RACF User News Or to see back issues: check Stu's website at http://www.stuhenderson.com/Newsletters-Archive.html

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.

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

Other Internet places:

- Nigel Pentland's security page iswww.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**