RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

This Issue's Theme:

- Make information security more effective and more efficient and more interesting.

Free Webinar: "*Mainframe Crypto for CIOs and the Rest of Us*" with Greg Boyd of Mainframe Crypto and Stu Henderson. To register: www.newera-info.com/Month.html

Sponsored by NewEra
May 23 and again June 1,at 2 pm EDT

This session is for CIOs, security administrators, system programmers, and auditors who have heard about cryptography (both hardware and the ICSF software with z/OS), know it's important, but don't really understand it.

You may have felt that other cryptography presentations went over your head. In this session, Greg and Stu tell you just what you need to know, in simple, understandable terms. You'll learn to cut expenses while improving security

----

NY Metro NASPA (National Association of System Programmers) Meets Wednesday, 26 April, **Room 1219, IBM Building, 590 Madison Avenue, NYC.** For free registration email Mark Nelson ("markan@us.ibm.com") with the subject "2017 April NASPA"

NEW YORK RUG Meeting Date

March 15,, 2017 from 10AM to near 4PM *at IBM in Tampa and NYC.*

THIS IS A LOT OF TRAINING AVAILABLE IN ONE DAY. **You will not be allowed to attend without pre-registering (it's free).** See inside for details. (The meeting after that will be **a Fall date to be determined in 2017**)

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: 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

" *If you are strong, you can be kind*."

– anonymous fisherman

Vanguard Conference

We are awaiting word on the Vanguard Security & Compliance for 2017.
For more information, please contact glory.wade@go2vanguard.com .

To subscribe to this newsletter, or for back issues:

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

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

Growing Need for Encryption Support

Several trends are pressing for greater mainframe support for encryption, all of which will affect RACF administrators and Data Security staff soon and hard. These trends include: new regulations from Federal, State, industry, and European regulators (please see article below on new regulations), new algorithms like AES, and new technology like the coming policy-based encryption for data at rest. The new RACF password encryption protocol KDFAES will require additional CPU resources. More and more, passwords will become obsolete and we will replace them with encryption based techniques to prove user identities.

So what should a RACF administrator or sysprog be thinking about?

- **ICSF** (Integrated Cryptologic Services Facility) is a started task that serves to route requests for encryption and decryption to the right hardware and software. You will want to have it up and running, with its own, protected, RACF userid.
- **Policy Agent** is another started task that lets you specify encryption policy for TCP/IP, for example: *"require this type of encryption on these ports from these IP addresses*" This is the easiest and most reliable method of providing encryption for TCP/IP on mainframes. You will want this up and running with its own, protected, RACF userid.
- **Policy based encryption for data at rest**. IBM has announced this as a coming feature in z/OS. Similar to Policy Agent, it lets us specify policy for automatic enforcement of encryption for data on tape and disk. You will want to be ready for this when it comes.
- **Key Management**. This will be extremely important since anyone who can see the decryption key can read and write data not otherwise protected. If you lose the keys, then you can't read or write it yourself. You will want to develop and enforce clear, tested, procedures for key management.
- The **CSFSERV and CSFKEYS and related resource classes** in RACF to control who can use encryption keys and who can make requests for encryption and decryption. You will need to be ready to implement these if you aren't already.
- **CPU capacity planning and tuning.** Encryption requirements will place additional demand on the CPU. You can avoid much of the additional cost by measuring and projecting relating demand; by making use of hardware features such as CPACF and CEX, and by controlling who is allowed to use encryption.
- **SMF Recording and Reporting**. For both security/audit monitoring and for CPU capacity planning, you will want to know who is using what encryption and decryption, and who is bypassing ICSF by coding her own encryption routines outside of the standard mechanisms. (Allowing encryption outside of the standard mechanisms makes CPU capacity planning more difficult.)
- **Organizational issues** You can't rely on just one sysprog or one RACF administrator to manage all the issues with encryption/decryption. You will want to have your organization: determine and enforce policy, assign responsibility, and provide sufficient resources.

Management Controls versus Passion

Which scenario do you think has better security: Scenario A or Scenario B?

Scenario A

A system programmer named George and a RACF administrator named Janet together decide how security options and rules are to be set. They work in a shop with very lean staff and do not have time to document the decisions they implement.

Scenario B

In a different shop, with a deeper bench, there is a formal policy specifying who is responsible for various aspects of information security, including risk assessments, approvals, re-certifications, audit liaison, compliance, network security, mainframe security, and distributed security, and more. Every rule and privilege and option set in RACF is formally approved in writing and re-certified annually. Every system software option is similarly approved in writing and re-certified annually. Several different teams of auditors annually review settings and permissions, comparing them to various checklists.

The answer might surprise you: Scenario A has just as much chance of having effective security as Scenario B. Piles of paperwork do not ensure security. Compliance without understanding of risk is wasted effort.

Some auditors have found that some data centers have lots of evidence of “compliance” without actually having good security.

There can be major advantages to having some of the paperwork in Scenario B, if it represents actual understanding of risk and meaningful steps to reduce it. Clear documentation can be useful when a key player retires and you need to know how options are supposed to be set. Clear documentation can reduce the effort for compliance management and dealing with auditors. It can accelerate development of effective new staff. Clear accountability for decisions can lead to more rigorous understanding of risks.

So how to tell where you stand? Two steps: first, estimate how much it costs your data center to handle compliance management and audit liaison. You will know immediately whether this cost is wasteful or not. Second, ask yourself whether you have clear information in writing to document how you do things. Sufficient information to continue functioning well after the loss of a key player? Sufficient information to hand to an auditor so it’s clear what the standards are and who is responsible for approving them, so the auditor doesn’t have to provide her own standard nor gather information that is irrelevant to the audit?

New York State Implements New Cybersecurity Regulations This March

We understand that they require: inventories of applications and data, formal risk assessments, encryption of data on the fly and at rest, and more. Some people expect other states to follow. Europe is getting new cybersecurity regulations this year (do you do business there?). Various Federal agencies have more regulations in the works. This is a good time to get to know your Legal and Compliance departments.

Getting Agreement on the Concept of “Privileged User”

At the last meeting of the NYRUG, several people described the advantages of having various people in your shop get agreement on what a “privileged” user is. Of course users with SPECIAL and OPERATIONS and perhaps AUDITOR and ROAUDIT come to mind. But perhaps also: userids with UID(0). Userids that are the OWNERs of production or system datasets and resources. Userids with CLAUTH(anything). Userids with group-SPECIAL or group-OPERATIONS. Userids that can access production or system datasets and resources. Userids connected to any group with AUTH other than USE. Userids which match the High Level Qualifier of production or system datasets. Userids for started tasks marked Trusted or Privileged.

More important than the conclusions you reach is the effect of various people discussing their opinions and reaching some sort of consensus on what “privileged” means in your shop. This will ideally lead to a consensus on who should have what privileges.

And then to decisions which of these should be subject to annual re-certification and by whom.

Meaningful Security Reports

If you want to be creative in a way that makes a difference, take a look at what reports would be useful for security administration in your data center. The starting point is the list of violations, which in many shops is a waste of paper and people’s time and effort. What exception reporting, pattern and identification, alerts of unusual spikes in activity, and interesting correlations would help improve security at low cost? As you will see below, financial fraud examiners use techniques we can borrow from.

Here are some ways to develop new types of useful reports, beyond the list of violations.

- Vary what you report.
  - Report on changes in number of users with SPECIAL, with OPERATIONS, with UID(0)
  - Instead of dataset accesses, report number of TCP/IP inbound messages from outside the firewall and from inside the firewall
  - Use of “firecall” or “break the glass” emergency privileged userids
  - Report the number of violations broken out by (production versus system versus other) and by (signon versus dataset access versus access by resource class)
  - Report accesses by started tasks that are only permitted because they are marked TRUSTED in the Started Procedures Table (see DSMON)

- Vary the types of item you report.
    - Instead of reporting violations, report successful accesses to datasets and resources, perhaps noting changes in the trend over time. What would it mean if unexpectedly a program reads the customer masterfile under a userid other than the production Marketing userid? Or if some month the Accounts Payable masterfile was updated 99 times more often than most months?
    - Or report the number of production dataset rules that have not been re-certified
    - Financial fraud examiners may report activity in accounts that haven't been accessed in a long time ("dormant accounts") on the theory that criminals might be targeting accounts of elderly customers who don't read their statements every month. A RACF administrator might want a report of activity on userids that previously hadn't been active in over a month.

- Vary the correlations between two or more items.
    - For example, financial fraud examiners might compare the number of purchase orders to the number of invoices received to the number of checks issued to pay invoices. What might a change in these ratios indicate?
    - Instead of reporting number of invoices etc., they might report dollar value of them. Or how often they occur. Or time of month or day of week

- Vary how you report it: listings, trends, exceptions, outliers, pie charts, bar charts, correlations (how well two numbers track with each other). Or just a one-line text stating that there is no significant change noted.

- Vary how often you have to look at the reports
    - Instead of a daily list of violations, receive one email per week listing the number and trend of violations
    - Receive a report only on an exception basis, that is when some type of event occurs more often than some definition of "normal"

Endangered Species: Passwords

Ten or twenty years from now, you may not be able to find any system using passwords to prove people's identities. This is because smart people, after a lot of thought and effort, have decided that passwords can't be relied upon. So you'll want to be getting ready for Two Factor (or Multi Factor) Authentication. You'll want also to start investigating other methods, methods that we're starting to see on Google, FaceBook, and other places. Some of these involve recognizing the computer you are signing on from (or the telephone number or IP address you are coming from) as one that has been established as trusted. Others rely on recognizing the patterns in which you hold and move your smart phone. Almost all of these rely on increased use of encryption.

Our Latest Checklist

We occasionally publish a list of items for you to consider when evaluating where you stand and what you want to do next to get your security where you want it to be. Here is a more advanced list of items to help you evaluate your RACF implementation. Few shops have addressed them all. How many of these have you accomplished? Which would you like to add to your to-do list?

___ Review the Healthchecks that IBM provides with z/OS and with RACF to determine which you want to use and how

___ Maintain an accurate inventory of hardware, software, applications, data, and networked connections

___ Develop and maintain written risk assessments for each application, to be used as the basis for deciding what protection is needed

___ Provide effective protection of your mainframe TCP/IP connections by means of Policy Agent, the SERVAUTH resource class, blocking of ports, and encryption

___ Assess cost savings from moving distributed apps to z/OS or z/VM (with LINUX running in guest machines)

___ Develop and enforce formal procedures for digital certificate management

___ Develop and enforce formal procedures for encryption management

___ Implement **ICSF** (Integrated Cryptographic Services Facility) in order to provide needed support for encryption at reasonable cost

___ Capacity planning and tuning for CPU usage for encryption

___ Establish the owner for each resource class, the person responsible for deciding whether to implement and how

___ Analytic reporting on RACF activity beyond just listing violations

Free Sources of Useful Guidance for InfoSec

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository

- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53

- Handouts from previous meetings of the NYRUG: http://www.nyrug.stuhenderson.com/handouts.HTM

- NewEra hosts free webinars on a variety of mainframe topics. You can see the schedule, and get handouts from previous sessions, at: http://www.newera-info.com/zwebs.html

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet March 15, 2017 from about 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa, a joint meeting by teleconference with the NY and Tampa FL RUGs.

Attendees **must present a government issued photo ID** to enter the IBM 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.
For Complete Directions, agenda, copies of handouts and to register, please visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.

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** (**$2195**)
December 5-8, 2017 in Bethesda, MD

2) HG05 **Advanced RACF Administration (\$2050)**
Dec. 11-14, 2017 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 9, 2017 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 z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)
Feb. 28-March 3, 2017 in Clearwater, Fl
September 25-28, 2017 in Chicago

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)
June 12-14, 2017 in Bethesda, MD
Nov. 15-17, 2017 in Bethesda, MD

C) HG76 **How to Audit UNIX and Windows Security (\$2200)**
October 24-27, 2017 in Bethesda, MD

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

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

For Back Issues of this Newsletter, Subscriptions and 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 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 s oftware and tape management software