21 Things You Didn't Used to Know About RACF

(A Technical Update for IT Auditors)

Stuart Henderson
The Henderson Group
(301) 229-7187

1

Here Are 21 Things Auditors Should Know About RACF

- One Person's Opinion, But You Need to be Aware of the Issues in Any Case
- And of Course, It's Easier When You Present Your Findings in the Light of the Specific Business Risk and Expected Cost to Reduce the Risk.

2

RACF is, of Course

- IBM's Resource Access Control Facility, the Software on IBM Mainframe Computers with the MVS Operating System That Checks Out Userids and Passwords, and Controls Who Can Access What Datasets (Files) and Resources.
- Market Leading Software Which Competes with ACF2 and TopSecret, Both from Computer Associates.

3

1) RACF Now Supports Mixed Case Passwords

- You Can Force Mixed Case with SETR
- To allow upper and lower case passwords for userids:
  - SETR PASSWORD(MIXEDCASE) and to undo it:
  - SETR PASSWORD(NOMIXEDCASE)
- (Don't turn this one on until you are sure you want it. It's very hard to turn it off after many users have entered passwords with lower case characters.)

4

1A) RACF Now Supports Mixed Case Passwords

To set new rules for passwords to accept upper and lower case letters in passwords:

SETR PASSWORD(RULE5 (LENGTH(6:8) ccc (1:8)))
where ccc is one of the new options: MIXEDCONSONANT, MIXEDVOWEL, or MIXEDNUM.

- To set a new minimum password change interval (for example, one day), issue:
  - SETR PASSWORD(MINCHANGE(1))

5

1B) RACF Now Supports Mixed Case Passwords

- Of course, You Shouldn't Activate This Until All Programs with Signon Screens Are Ready, and Users Are Properly Trained
- For More Info Please See Issue 67 of the RACF User News at:

www.stuhenderson.com/XRUGNTXT.HTM

6

2) RACF Now Supports Long Password Phrases as Well as Passwords

- **Here is the Syntax to Add a Password Phrase to a User Record:**

```
ALU USER02                                    +
     PHRASE                                   +
     ('July14IsBastilleDayLikeJuly4, ButInFrance')
```

- **Password Phrases Can Have Length of 14-100 Characters. Use Exit to Make This 9-100.**

7

2A) RACF Now Supports Password Phrases as Well as Passwords

- **Can't Contain the Userid (uppercase or lowercase, or mixed)**
- **Must contain**
  - **at least 2 alphabetic characters (A–Z, a–z)**
  - **at least 2 non-alphabetic characters (numerics, punctuation, or special characters)**
  - **not more than 2 consecutive identical characters that are identical**
- **For More Info Please See Issue 69 of the RACF User News at:**
  www.stuhenderson.com/XRUGNTXT.HTM

8

3) RACF's Erase On Scratch Function No Longer Has Performance Problems

- **New Hardware Features in Disk Drives, Plus Electronic Caching in Control Units Have Solved the Old Performance Problem.**
- **RACF Lets You Turn On EOS One Dataset at a Time.**

9

4) You Need to Audit RACF with Tape Management Software

- **Problems Include:**
  - **17 Character DSNAME problem**
  - **Residual Data**
  - **Bypass Label Processing**
  - **PROTECTALL with Foreign Tapes**

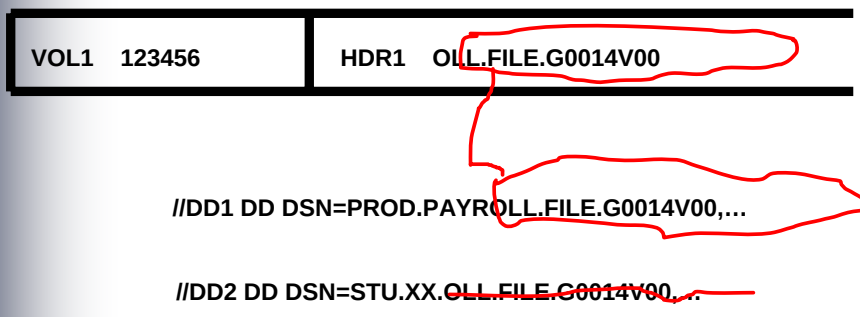
10

4A) You Need to Audit RACF with Tape Management Software

- **New Parmlib Options in Member DEVSUPxx Make This Much Easier:**
  - **TAPEAUTHDSN**
  - **TAPEAUTHFC1**
  - **TAPEAUTHRC4**
  - **TAPEAUTHRC8**
- **With the TMS, These Let You Turn On PROTECTALL, Protect Tapes, and Allow Foreign Tapes, and Control Multi-File Tapes**

11

4B) OPEN Makes Two Checks for SL Tapes



1) Compare DSNAME in Label Against DD Card

2) Call RACF with RACHECK

12

4C) You Need to Audit RACF with Tape Management Software

- **And While You're At It, You Might Address**
  - **Tape Dataset Encryption,**
  - **Key Management, and the**
  - **New Encrypting Tape Drives.**
- **For More Info, Please See the Article at**

http://www.stuhenderson.com/TAPESEC1.PDF

13

5) The Program Named AMASPZAP No Longer Needs to Be Protected

- **Despite What Some Audit Checklists Say. IBM has Rewritten It Completely to Remove the Security Problem**
- **How Should the RACF Administrator Determine Which Programs to Protect?**

14

5A) The Program Named AMASPZAP No Longer Needs to Be Protected

- For More Info, Check This IBM Manual in the Chapter on SPZAP in the Section Called Operating Considerations:

Manual Number: GA22-7589-10 "z/OS V1R8.0 MVS Diagnosis Tools and Service Aids"

- You Can Download it For Free From:

http://publibz.boulder.ibm.com/epubs/pdf/iea2v170.pdf

15

6) Two Resource Classes Tell You Differently Whether They Are Active

- For the PROGRAM Class, Look at the First Line of SETR LIST for Some Version of:

  WHEN(PROGRAM)

- Tells You That the PROGRAM Class is Active.

16

6A) Two Resource Classes Tell You Differently Whether They Are Active

- For the GLOBAL Class, Check the DSMON Global Access Table Report

17

7) IBM Gives Us UNIX Under the Control of MVS (Called USS)

- It's Hard to Turn It Off.
- It Uses RACF for Security.
- It's the Most Secure, Most Standard, Most Reliable, Most Scalable UNIX You'll Find Anywhere.

18

7A) IBM Gives Us UNIX Under Control of MVS for Free (Called USS)

- You Should Address It in a Separate Audit.
- It Replaces /etc/passwd with RACF

19

8) RACF Secures the Free TCP/IP IBM Gives Us with MVS and USS

- You Should Address It in a Separate Audit.
- Get a Copy of the TCP/IP Control File for Your Work Papers
- You Can for Example Use RACF to Control Access to Ports and to IP Addresses.

20

8A) RACF Secures the Free TCP/IP IBM Gives Us with MVS and USS

- Get to Know the SERVAUTH Resource Class in RACF
- It Lets You Control Access to IP Addresses, Ports, and Other Network Resources in RACF
- The Policy Agent Software Provides Firewall-Like Services, Such as Packet Filtering and Intrusion Detection

21

9) RACF Secures the TCP/IP Daemons Such as FTP, Telnet, etc.

- Should Be Addressed in a Separate Audit
- Get the Control File for Each Daemon In Scope
- To Learn What Daemons Are Active, Issue the TSO Command NETSTAT. (It's Like the NETSTAT You Know from UNIX and Windows.)

22

10) FTP on the Mainframe Needs Extra Attention Because:

- It Can Be Used to Upload and Download both USS Files and MVS Datasets.
- It Can Access Print Files on the Spool
- It Can Talk To DB2
- It Can Submit Batch Jobs to JES. (The RACF Switch BATCHALLRACF Becomes More Important Now.)

23

11) Telnet on the Mainframe Needs Extra Attention Because:

- It Can Be Used to Sign Onto Any Applid (like CICS or TSO), Not Just to USS).
- It Opens the Mainframe World to the Internet

24

11B) Telnet on the Mainframe Needs Extra Attention Because:

- It Increases the Need to Make Sure That Every Applid Calls RACF to Check Out the Userid and Password.
- Its Control File Can Restrict What Applids You Can Telnet To (See ALLOWAPPL)
- The Control File Can Also Be Used to Provide SSL Encryption with TCP/IP

25

12) Mainframes Software (CICS, DB2, MQ, Others) Talk Over the Internet

- Guess what: Separate Audits
- Each of These (CICS etc) Has a Control File That Can Specify SSL Encryption Over the Internet

26

13) RACF Secures the Mainframe Web Server (httpd)

- Comparable to Apache on UNIX or IIS on Windows
- Can Log Internet Users on Without a Password
- Should be a Separate Audit
- Control File Can Specify SSL Encryption Over the Internet and How Users Are ID'd

27

14) RACF Userids Can Have the RESTRICTED Attribute

- This Prevents the Userid From Gaining Access to Data or a Resource by Means of the UACC, or the Global Access Table or ID(*) Permission
- Designed for Userids Logged on with the Web Server to Limit Their Access to Just What They Are Explicitly Allowed

28

15) RACF Userids Can Have the Protected Attribute

- Which Means They Have No Password and Can Only Be Used with Automatic Logons
- Designed for Use with All Started Tasks, All Production Batch Jobs, and Preset Terminal Security in CICS

29

16) SNA is Here to Stay, And Needs to Be Secured

- Ask The VTAM System Programmer
  - the Name of Your APPN Network,
  - the Names of the Networks It Connects to, And
  - the Names of the Networks They Connect To
- Many VTAM Parameters Involved. See SYS1.VTAMLST

30

16A) SNA is Here to Stay, And Needs to Be Secured

- RACF Resource Classes: APPCLU and VTAMAPPL
- A Separate Audit of Course
- For More Info, Please See www.net-q.com

31

16) RACF Should Be Used to Protect NJE and RJE

- (NJE is Network Job Entry; RJE is Remote Job Entry. Both Allow Batch Jobs, Printouts, and Operator Commands to Be Sent Over Phone Lines to Your Mainframe)
- Paths Into the System
- Protect with NODES, WRITER, FACILITY, and JESINPUT Resource Classes and BATCHALLRACF

32

16A) RACF Should Be Used to Protect NJE and RJE

- Other Organizations Can Submit Batch Jobs, Operator Commands, and Printouts Over NJE or RJE.
- Learn Names and Locations from JES System Programmer

33

17) OPERCMDS Resource Class Restricts Operator Commands

- MVS, JES, and Other Operator Commands
- Commands Can Be Entered at Consoles, But Also in Batch Jobs, in Parmlibs, From Programs, TSO, NJE, and RJE

34

18) The JESSPOOL Resource Class Protects Data in Printouts

- Data Can Otherwise Be Browsed by Unauthorized Users from Many Different Programs Such as SDSF and FTP
- SDSF Functions Can Be Further Restricted with the SDSF Resource Class in RACF

35

19) The VTAMAPPL Resource Class Protects VTAM Applids

- Risk of Some User Writing a Program That Spoofs an Applid, Uses It to Harvest Userids and Passwords
- Easy to Implement

(An applid is of course a program like CICS or TSO that lets a user talk to it from a terminal, that is: a program with a signon screen)

36

20) Some Shops Have Two, One or Even Zero OPERATIONS Userids

- (Excepting of Course IBMUSER, Which Should Be Revoked)
- Use of FACILITY Class Rules with Names Starting STGADMIN.
- DASDVOL Resource Class
- Firecall Userids

37

20A) Some Shops Have Two, One or Even Zero OPERATIONS Userids

In Google, Type the Keywords RACF, Stinkin, and OPERATIONS to find presentations showing how.

- Less Need for OPERATIONS When IPLs Occur Only Once Every Few Months
- How Would You Handle an Audit with 17 OPERATIONS Userids?

38

20B) Some Shops Have Two, One or Even Zero OPERATIONS Userids

- Of Course, There is No Correct Number of OPERATIONS Userids.
- So an Auditor Would Look to See Who is Responsible for Approving Who Gets OPERATIONS (and SPECIAL), How It Is Documented, and How the Approval Forms Match the RACF Rules: How is the Decision Made and Who is Responsible

39

21) Senseless to Ask RACF Admin to "Review the Violations Report"

- What Should He Do with a Violation? He Has No Authority to Change Others' Behavior
- Not Fair to Make Him Responsible When He Doesn't Have the Authority to Do Anything About It. A Recommendation That Irritates Auditees, Since It Takes Time and Effort, But Makes No Difference
- More Important to Look for Trends, Patterns, Clusters

40

21A) Senseless to Ask RACF Admin to "Review the Violations Report"

- "You Can't Manage It If You Don't Measure It"
- Trend Over Time of Invalid Passwords Per Day, Other Measures

41

22) Next Release of RACF and z/OS (1.11) Has Important New Features

- Digital Signatures and Verification of Program Modules to Identify Unauthorized Modifications (Effect on Change Control Audits)
- More Health Checker Checks
- New Identity Propagation Function to Associate Distributed Identities with RACF Userids

42

We Hope This Has Added to Your RACF Audit Knowledge

- **I Welcome Your Comments, Questions, Suggestions:**

  (301) 229-7187
  stu@stuhenderson.com

- **"The Best Auditing is a Form Of Consulting"**