The ABCs of Auditing SecureWay Security Server

(the security system formerly known as RACF)

Mark S. Hahn, mhahn@us.ibm.com
Consultant, IBM Corporation
ISACA Toronto, Canada
March 22, 2001

Disclaimers

The following are trademarks or registered trademarks of the International Business Machines Corporation:

MVS/ESA

OpenEdition

OS/390

RACF

UNIX is a registered trademark in the United States and/or other countries, licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Wherever RACF is mentioned, other products providing comparable services may be used.

This reflects the experience of the presenter. Your experience (and mileage) may vary.

Objectives

- Use of basic tools
  - DSMON
  - SETROPTS LIST
  - Basic RACF commands
  - RACF subsystem
  - RACFRW / IRRADU00
- Ensure control settings are appropriate to environment
- Accurate documentation of live system settings

What is RACF*

- Resource Access Control Facility
  - Component of OS/390 and z/OS
  - Security server tied to OS/390, generally even releases
    Security Server 2.4 in OS/390 2.4
    Security Server 2.6 in OS/390 2.7
  - Audit log generator
  - Makes recommendations when called, passive system

* OS/390 has renamed RACF to the security server. Terminology is equivalent.

Functions of RACF

- Control system entry
  - userid and password verification
  - applications
- Control resource access
  - Data sets
  - Services and facilities
- Optional: journal security events

Information Collection

- System Access
  - Either an AUDITOR userid
  - Co-operative security / sysprog
- Data collection
  - SYSOUT listings
  - Output to data set: eMail or FTP

Jobstream

- Verify environment
  - LISTUSER userid
    - Userid have AUDIT?
  - RVARY LIST
    - Determine RACF dataset(s)
  - Full DSMON report
  - SETROPTS LIST
    - Determine RACF environment

Job Stream

```
//jobn JOB (acct),'AUDIT'
//TSO  EXEC  PGM=IKJEFT01
//SYSPRINT DD SYSOUT=*
//SYSTSPRT DD DSN=data.set, …
//SYSTSIN  DD *
LISTUSER userid
RVARY LIST
SETROPTS LIST
```

D S M O N

Setup

- Authorization
  - System AUDITOR
  - Program control access ICHDSM00
- JCL

```
//jobname JOB …
//DSMON  EXEC  PGM=ICHDSM00
//SYSPRINT  DD  SYSOUT=*
//SYSUT1    DD  DSN=SYS1.PARMLIB
//SYSOUT    DD  SYSOUT=*
```

Using DSMON

- System report
- Group-tree report
- Program-properties table report
- RACF authorized-caller table report
- RACF class-descriptor table report
- RACF exits report
- RACF global-access-checking table report
- RACF started-procedures table report
- Selected user-attribute report
- Selected user-attribute summary report
- Selected data-sets reports (for SYS1.PARMLIB, authorized program facility libraries, master and user catalogs, primary and backup RACF databases, and user-defined data sets).

System Environment

```
RACF DATA SECURITY MONITOR    DATE: 01/09/01  TIME: 09:36:39  PAGE  1
                             S Y S T E M     R E P O R T
-------------------------------------------------------------------
CPU-ID                                 110521
CPU MODEL                              500
OPERATING SYSTEM/LEVEL                 MVS/ 3.8   SP6.0.5 HBB6605
SYSTEM RESIDENCE VOLUME                RESA11
SMF-ID                                 SYS1
0RACF VERSION 2 RELEASE  4.0 IS ACTIVE
```

- Basic system identification information
- Note: OS/390 R2.5; security server at 2.4

Program Properties Table (PPT)

```
P R O G R A M     P R O P E R T I E S     T A B L E     R E P O R T
PROGRAM           BYPASS PASSWORD         SYSTEM
 NAME              PROTECTION              KEY
 ------------------------------------------------------------------
IEDQTCAM                NO                   YES
ISTINM01                YES                  YES
IKTCAS00                NO                   YES
AHLGTF                  NO                   YES
```

- Formats system merged copy of IEFSDPPT and SCHEDxx parmlib member.
- Reports on programs able to
  - bypass RACF protection
  - execute in storage key < 8 and gain system state

PPT (continued)

- Unanswered questions
  - What is the program? What is ISTINM01?
  - What are acceptable settings for those parameters?
  - What is source of definitions: IBM or installation?
  - Is there significance to order of entries?
- Forces auditor to review parmlib(SCHEDxx) member
- Look for unrecognized entries and carefully review those.

PPT Review (SCHEDxx)

- Review installation definitions
- Keyword syntax

```
 BROWSE    SYS1.PARMLIB(SCHED00) - 01.00
 Command ===>
******************** Top of Data ****
MT SIZE(64K)
PPT PGMNAME(EPWINIT) NOCANCEL NOSWAP KEY(0)
    NODSI NOPASS NOPREF
PPT PGMNAME(IRRSSM00) NOCANCEL NOSWAP KEY(2)
    PRIV SYST
PPT PGMNAME(EZAPPFS) NOSWAP KEY(1)
PPT PGMNAME(EZAPPAAA) NOSWAP KEY(1)
```

Authorized Caller Table

```
R A C F     A U T H O R I Z E D     C A L L E R     T A B L E
R E P O R T
MODULE                RACINIT         RACLIST
NAME                  AUTHORIZED      AUTHORIZED
 ------------------------------------------------------------
NO ENTRIES IN RACF AUTHORIZED CALLER TABLE
```

- Formats contents of ICHAUTAB load module.
- Lists programs (in ANY library) able to issue RACINIT or RACLIST calls.
- Should be empty.

R A C F E x i t s

```
                    R A C F   E X I T S   R E P O R T
EXIT MODULE         MODULE
 NAME               LENGTH
 ------------------------------------------------------------------------------------------------------------
NO RACF EXITS ARE ACTIVE
```

- RACF exits which are active - name must match in Link Pack Area.
- This is also reported on console message when RACF initiates.

Powerful Users Report (L)

```
S E L E C T E D    U S E R    A T T R I B U T E    R E P O R T

USERID           ----------------- ATTRIBUTE TYPE -----------------
                 SPECIAL         OPERATIONS     AUDITOR         REVOKE
-------------------------------------------------------------------------
BHJZGD4                            SYSTEM         SYSTEM         SYSTEM
BHOOWHE          GROUP
BHSVIOF                                                           SYSTEM
```

- Lists users with special privileges or REVOKEd
- List of non-REVOKEd users “should” be small
- List of REVOKEd users varies by policy.
- Watch users with multiple privileges.

Powerful Users (R)

```
I B U T E     R E P O R T
 -------------  ASSOCIATIONS  -------------
 NODE.USERID          PASSWORD   ASSOCIATION
                      SYNC       TYPE
-----------------------------------------
 ARP1.SYSMSH2         NO         PEER
 ARP1.SYSRBB2         NO         PEER
 ARP1.SYSRBB          NO         PEER
```

Powerful User Summary

TOTAL DEFINED USERS: 2,684
TOTAL SELECTED ATTRIBUTE USERS:

ATTRIBUTE BASIS	SPECIAL	OPERATIONS	AUDITOR	REVOKE
SYSTEM	7	18	3	408
GROUP	11	0	2	4

- Review the numbers
- Make sense to you?

S T A R T E D Class

```
FROM PROFILES IN THE STARTED CLASS:
-----------------------------------------------------------
PROFILE          ASSOCIATED  ASSOCIATED
NAME               USER        GROUP     PRIV  TRUST  TRACE
-----------------------------------------------------------
BPXOINIT.* (G)   OMVSKERN    OMVSGRP     NO    NO     NO
BPXSTOP.* (G)    OMVSKERN    OMVSGRP     NO    NO     YES
. . .
SYNRECAL.* (G)   FDR         SYSPROG     NO    NO     YES
SYSLOGD*.* (G)   OMVSKERN    OMVSGRP     NO    NO     YES
TCPIP.* (G)      TCPIP       OMVSGRP     NO    NO     YES
*.* (G)          STARTED     SYSPROG     NO    YES    YES
```

Started Task Analysis

```
RACF DATA SECURITY MONITOR DATE: 01/09/97  TIME: 20:55:51  PAGE: 9
R A C F  S T A R T E D  P R O C E D U R E S  T A B L E  R E P O R T
FROM THE STARTED PROCEDURES TABLE (ICHRIN03):
 ------------------------------------------------------------------
PROCEDURE       ASSOCIATED      ASSOCIATED
 NAME            USER            GROUP          PRIVILEGED TRUSTED
 ------------------------------------------------------------------
JESA            SYSJES2         SYSSTC            YES       NO
VTAMUITW        SYSVTAM         SYSSTC            YES       NO
CNMPROC         SYSCNM          SYSSTC            NO        NO
CNMPSSI         SYSCNM          SYSSTC            NO        NO
REST            RCBBRST         SYSOPR            NO        NO
*               =                                 NO        NO
```

- Merge of installation ICHRIN03 table and STARTED class entries.
- TRUSTED preferred to PRIVILEGED
- Shared userids possible (no password checking)
- Generic entry is final, by definition.

Started Task Analysis

Checklist

- why PRIVILEGED? TRUSTED preferred
- Convert from ICHRIN03 to STARTED class when possible.
  - Dynamic updates w/o IPL
  - English instead of bits
  - No need to count entries (or have assembler do it).
- Watch SYSLOG for assignment of userid to started task (via TRACE(YES))
  - Should be on generic entry, others as desired.

Class Descriptor Table

```
RACF DATA SECURITY MONITOR DATE: 01/09/97  TIME: 20:55:51     PAGE:  31
R A C F    C L A S S    D E S C R I P T O R    T A B L E    R E P O R T
CLASS                                          DEFAULT  OPERATIONS
NAME          STATUS    AUDITING    STATISTICS    UACC     ALLOWED
-------------------------------------------------------------------
RVARSMBR      ACTIVE      YES           NO        NONE       NO
RACFVARS      ACTIVE      YES           NO        NONE       NO
SECLABEL      INACTIVE    YES           NO        NONE       NO
```

- VERY RACF release dependent
- No sorted order
- STATUS: ACTIVE if in use, INACTIVE is okay
- AUDITING: should be YES
- STATISTICS: should be NO, unless specific needs

RACF Class Descriptor Table (CDT)

- Merge of two RACF CSECTs:
  - IBM's default table (ICHRRCDX)
  - Installation's usermod (ICHRRCDE)
    - Should have #$@ or 0-9 in first 4 positions
    - e.g. $$OMCAN
  - No indication of which is whose

MVS Router Table

- Merge of two tables: IBM's and installation.
- No native audit tool.
- If CDT entry not matched with router table entry – class is inactive, even if RACF thinks / says it is active.

Data Set Analysis

S E L E C T E D D A T A S E T S R E P O R T

DATA SET NAME	VOLUME SERIAL	SELECTION CRITERION	RACF INDICATED	RACF PROTECTED	UACC
SYS1.LPALIB	RESA11	SYSTEM	NO	YES	READ
SYS1.MIGLIB	RESA11	LNKLST	NO	YES	READ
SYS1.NUCLEUS	RESA11	SYSTEM	NO	YES	READ
SYS1.PARMLIB	MCATA1	SYSTEM	NO	YES	READ
SYS1.PROCLIB	MCATA1	SYSTEM	NO	YES	READ
SYS1.SBDTCMD	RESA11	APF	NO	YES	READ
SYS3.RACF.BACK	RACFX2	RACF BACKUP	NO	YES	NONE
SYS3.RACF.PRI	RACFX1	RACF PRIMARY	NO	YES	NONE
CATALOG.MCATA1	MCATA1	MASTER CATALOG	NO	YES	READ
CATALOG.VMPM001	OSSYS6	USER CATALOG	NO	YES	UPDATE

Data set Analysis Notes

- RACF data bases
- Master Catatlogs
- User Catalogs
- NF data sets
- NM data sets

RACF Data Base Protection

- Review profile protecting RACF data base
  - LISTDSD DA('racf.dataset.name')
    - What is UACC / ID(*)?
    - Who is on access list, with what authority?
      - UPDATE may be needed for IRRDBU00 or other product usage
    - Are backups made? If not, why not?
      - What is protection on backups?
    - Bonus: primary / backup widely separated?

Master / User Catalogs

- Master Catalog
  - UACC(READ)
  - SYSTEMS / Tech Support: UPDATE
  - DASD management: ALTER
- User Catalog
  - UACC(UPDATE)
  - DASD management: ALTER

NF / NM Data sets

- NF – Not Found
  - Data set not where it supposed to be
  - Correct the problem
- NM – DASD volume not mounted
  - ?Who has mountable volumes?
  - Correct the problem

p a r m l i b

- Multiple data sets
- Defined in LOADxx member of IPLPARM or SYS1.PARMLIB
- Operator command: D PARMLIB
- Ensure all are protected
- Sequence counts – may segregate who has which
- Review members, especially SORT CHANGED on SPF directory listing

RACF parmlib

- NOT related to system parmlib
- MUST be protected against update and audited for changes
- Defined in RACF proc within SYS1.PROCLIB
- Review members, especially SORT CHANGED on SPF directory listing

H F S

- Hierarchical File System
  - UNIX System Services data sets
    - More in Audit UNIX session
  - What to name? How to protect?
    - System resource, not user
    - DSN should NOT start w/userid
    - UACC(NONE); only OMVS to update
  - Defined in parmlib(BPXPRM0F) or operator D OMVS,F
  - Recommended: SMS-managed

SETROPTS LIST

SETROPTS Analysis

```
ATTRIBUTES = INITSTATS WHEN(PROGRAM) SAUDIT CMDVIOL
   NOOPERAUDIT
```

- Some items not visible without AUDITOR privilege: SAUDIT, OPERAUDIT, CMDVIOL
- Attributes =
  - **INITSTATS** - keep track of RACINITs
    Plays a role in password aging and idle userid revocation
  - WHEN(PROGRAM) - activate PADS
  - **SAUDIT** - Audit commands authorized via SPECIAL privilege
  - **CMDVIOL** - Audit command violations
  - **OPERAUDIT** - Audit resource accesses authorized by OPERATIONS privilege

S E T R O P T S 2

```
STATISTICS = NONE
AUDIT CLASSES = NONE
```

- Statistics
  - Only kept for Discrete (non-Generic) profiles
- Audit Classes =
  - Ideally should be all classes, active or not.
  - Tracks changes to profiles within RACF database, not accesses to resources. Supplements SAUDIT.

SETROPTS 3

```
ACTIVE CLASSES = DATASET USER GROUP RVARSMBR RACFVARS TAPEVOL TCICSTRN
                 GCICSTRN PCICSPSB QCICSPSB GLOBAL GMBR FACILITY FCICSFCT
                 HCICSFCT JCICSJCT KCICSJCT DCICSDCT ECICSDCT SCICSTST
                 UCICSTST MCICSPPT NCICSPPT ACICSPCT BCICSPCT TSOPROC
                 ACCTNUM TSOAUTH FIELD CCICSCMD VCICSCMD APPCLU OPERCMDS
                 JESSPOOL JESJOBS CONSOLE SURROGAT NODMBR NODES SDSF GSDSF
                 APPCSERV PTKTDATA PTKTVAL STARTED RRSFDATA
```

- Documents classes for which RACF will lookup profiles (assuming Router table entry).
- Should only be those for which services are in use.
- Sequence is IBM (approximately order introduced) followed by user.
- Merged list
- Includes member classes and grouping class
- Some classes need preparation before activating.

SETROPTS 4a

```
GENERIC PROFILE CLASSES =  DATASET RVARSMBR RACFVARS SECLABEL DASDVOL
                           TAPEVOL TERMINAL APPL TIMS AIMS TCICSTRN PCICSPSB
                           GMBR DSNR FACILITY VMMDISK VMRDR VMCMD VMNODE
                           VMBATCH SCDMBR FCICSFCT JCICSJCT DCICSDCT SCICSTST
                           MCICSPPT ACICSPCT PMBR TSOPROC ACCTNUM PERFGRP
                           TSOAUTH MGMTCLAS STORCLAS FIELD CCICSCMD VMBR
                           PROPCNTL APPCLU SMESSAGE DEVICES VTAMAPPL PSFMPL
                           OPERCMDS WRITER JESSPOOL JESJOBS JESINPUT CONSOLE
                           SURROGAT NODMBR NODES PIMS SIMS FIMS OIMS NVASAPDT
                           VXMBR CIMS DLFCLASS SDSF CSFSERV CSFKEYS APPCTP
                           APPCSI APPCPORT RMTOPS INFOMAN RODMMGR MQQUEUE
                           MQPROC MQNLIST MQADMIN MQCMDS MQCONN NETCMDS
                           NETSPAN SUBSYSNM CPSMOBJ CPSMXMP RACGLIST PTKTDATA
                           LFSCLASS MQCHAN DBNFORM IBMOPC LOGSTRM PTKTVAL
                           STARTED RRSFDATA SYSMVIEW VMSEGMT VMMAC TEMPDSN
                           DIRAUTH DIRSRCH DIRACC FSOBJ FSSEC PROCESS
                           PROCACT
```

SETROPTS 4b

```
GENERIC COMMAND CLASSES =  DATASET RVARSMBR RACFVARS SECLABEL DASDVOL
                           TAPEVOL TERMINAL APPL TIMS AIMS TCICSTRN PCICSPSB
                           GMBR DSNR FACILITY VMMDISK VMRDR VMCMD VMNODE
                           VMBATCH SCDMBR FCICSFCT JCICSJCT DCICSDCT SCICSTST
                           MCICSPPT ACICSPCT PMBR TSOPROC ACCTNUM PERFGRP
                           TSOAUTH MGMTCLAS STORCLAS FIELD CCICSCMD VMBR
                           PROPCNTL APPCLU SMESSAGE DEVICES VTAMAPPL PSFMPL
                           OPERCMDS WRITER JESSPOOL JESJOBS JESINPUT CONSOLE
                           SURROGAT NODMBR NODES PIMS SIMS FIMS OIMS NVASAPDT
                           VXMBR CIMS DLFCLASS SDSF CSFSERV CSFKEYS APPCTP
                           APPCSI APPCPORT RMTOPS INFOMAN APPCSERV RODMMGR
                           MQQUEUE MQPROC MQNLIST MQADMIN MQCMDS MQCONN
                           NETCMDS NETSPAN SUBSYSNM CPSMOBJ CPSMXMP RACGLIST
                           PTKTDATA LFSCLASS MQCHAN DBNFORM IBMOPC LOGSTRM
                           PTKTVAL STARTED RRSFDATA SYSMVIEW VMSEGMT VMMAC
                           TEMPDSN DIRAUTH DIRSRCH DIRACC FSOBJ FSSEC
                           PROCESS PROCACT
```

SETROPTS 4c

- Source of confusion
- GENERIC PROFILES should equal GENERIC COMMANDS.
- GENERIC PROFILES interpret ‘*’ as masking, (G)eneric
  - BEFORE activating GENERIC for a class, look for any profiles with masking, remove before activating GENERIC.
- GENERIC COMMANDS process (G)eneric profiles.

SETROPTS 5

```
GENLIST CLASSES =  NONE
GLOBAL CHECKING CLASSES =  DATASET
SETR RACLIST CLASSES =  RACFVARS FACILITY TSOPROC ACCTNUM TSOAUTH FIELD
                        OPERCMDS NODES PTKTDATA PTKTVAL STARTED
GLOBAL=YES RACLIST ONLY =  TCICSTRN SCICSTST
```

- Related to performance - storage location of profiles - mutually exclusive
- GENLIST
  Anchor generics in requestor's address space - controlled by CDT definition
- GLOBAL CHECKING
  Can only allow (non-allow forces regular checking), no tracking of allowed accesses, fastest check performed – carefully review (DSMON, later)
- RACLIST
- GLOBAL RACLIST

SETOPTS 6a

```
LOGOPTIONS "ALWAYS" CLASSES =  NONE
LOGOPTIONS "NEVER" CLASSES =  NONE
LOGOPTIONS "SUCCESSES" CLASSES =  NONE
LOGOPTIONS "FAILURES" CLASSES =  NONE
LOGOPTIONS "DEFAULT" CLASSES =  DATASET RVARSMBR RACFVARS SECLABEL DASDVOL
                                GDASDVOL TAPEVOL TERMINAL GTERMINL APPL
                                TIMS GIMS AIMS TCICSTRN GCICSTRN PCICSPSB
                                QCICSPSB GLOBAL GMBR DSNR FACILITY VMMDISK
                                VMRDR VMCMD VMNODE VMBATCH SCDMBR SECDATA
                                FCICSFCT HCICSFCT JCICSJCT KCICSJCT DCICSDCT
                                ECICSDCT SCICSTST UCICSTST MCICSPPT NCICSPPT
                                ACICSPCT BCICSPCT PMBR PROGRAM TSOPROC
                                ACCTNUM PERFGRP TSOAUTH MGMTCLAS STORCLAS
                                FIELD CCICSCMD VCICSCMD VMBR VMEVENT PROPCNTL
                                APPCLU SMESSAGE DEVICES VTAMAPPL PSFMPL
                                OPERCMDS WRITER JESSPOOL JESJOBS JESINPUT
                                CONSOLE SURROGAT NODMBR NODES PIMS QIMS
                                SIMS UIMS FIMS HIMS OIMS WIMS NVASAPDT
                                VXMBR VMXEVENT CIMS DIMS DLFCLASS SDSF
                                GSDSF CSFSERV CSFKEYS GCSFKEYS APPCTP
                                APPCSI APPCPORT RMTOPS INFOMAN GINFOMAN
                                APPCSERV RODMMGR MQQUEUE GMQQUEUE MQPROC
                                GMQPROC MQNLIST GMQNLIST MQADMIN GMQADMIN
                                MQCMDS MQCONN NETCMDS NETSPAN SUBSYSNM
                                CPSMOBJ GCPSMOBJ CPSMXMP RACGLIST PTKTDATA
                                LFSCLASS MQCHAN GMQCHAN DBNFORM IBMOPC
                                LOGSTRM KEYSMSTR DCEUUIDS PTKTVAL STARTED
                                RRSFDATA SYSMVIEW CBIND SERVER SOMDOBJS
                                VMPOSIX FILE DIRECTRY SFSCMD ALCSAUTH
                                VMSEGMT VMMAC TEMPDSN DIRAUTH DIRSRCH
                                DIRACC FSOBJ FSSEC PROCESS PROCACT IPCOBJ
```

SETROPTS 6b

- Logging Options
  - Not visible without AUDITOR privilege
  - Supplements the profile logging options (e.g. AUDIT(FAILURE(ALTER))
  - ALWAYS
  - NEVER
  - SUCCESS
  - FAILURES
  - DEFAULT

S E T R O P T S 7

```
AUTOMATIC DATASET PROTECTION IS NOT IN EFFECT
ENHANCED GENERIC NAMING IS IN EFFECT
REAL DATA SET NAMES OPTION IS INACTIVE
```

- NOADSP
  - Deactivates ADSP in userid or in group connection or PROTECT=YES in JCL.
  - Refuses to automatically create discrete profiles.
- EGN
  - applies to data set profiles.
  - Should be yes.
- REALDSN
  - Place translated (Naming Conventions table, single prefix) data set names into event records.

S E T R O P T S 8

```
JES-BATCHALLRACF OPTION IS ACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL IS ACTIVE, CURRENT OPTIONS:
   PROTECT-ALL FAIL OPTION IS IN EFFECT
```

- JES options
  - BATCHALLRACF - all batch jobs must be assigned userid.
  - XBMALLRACF - Execution Batch Monitor - seldom used.
  - EARLYVERIFY - ignored as of JES 3.1.3
- PROTECT-ALL FAIL favored
  No profile - no access.
  WARN for migration (SHORT term)

SETROPTS 9

```
 TAPE DATA SET PROTECTION IS INACTIVE
 SECURITY RETENTION PERIOD IN EFFECT IS     0
DAYS.
 ERASE-ON-SCRATCH IS INACTIVE
 SINGLE LEVEL NAMES NOT ALLOWED
```

- TAPEDSN
  Use of TAPEDSN protects data sets on tape same as on DASD.
- RETPD
- EOS
  - overrides profile specification
- Data set names must have hlq.

SETROPTS 10

```
 LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
 INACTIVE USERIDS ARE BEING AUTOMATICALLY REVOKED AFTER
90 DAYS.
 NO DATA SET MODELLING BEING DONE.
```

- List of Groups removes Default group restriction
- Idle userids
  - requires INITSTATS
  - SPECIAL userid protected
  - Review inactive userids (SEARCH CLASS(USER) AGE(nn) command)
- Data set modeling
  - Seldom used – generics
  - canned profile based on user, group or dataset

SETOPTS 11

```
PASSWORD PROCESSING OPTIONS:
   PASSWORD CHANGE INTERVAL IS  30 DAYS.
   32 GENERATIONS OF PREVIOUS PASSWORDS BEING
MAINTAINED.
   AFTER   5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
       A USERID WILL BE REVOKED.
   PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
   NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.
```

- How long is password good? <s/b short>
- How many old passwords kept <some>
- How many tries before REVOKE?
- How many days warning of password expiration (why?)
- Syntax rules good and bad:
  - can force minimum length
  - require at least one numeric, anywhere
  - make it easier to crack if specific characters is specific locations.

S E T R O P T S 1 2

```
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

- The RVARY passwords should NEVER be set to default.
- Review password storage, documentation procedures.

SETROPTS 13

```
SECLEVELAUDIT IS INACTIVE
SECLABEL AUDIT IS NOT IN EFFECT
SECLABEL CONTROL IS NOT IN EFFECT

GENERIC OWNER ONLY IS NOT IN EFFECT
```

- Security labels / Levels not generally used.
- Generic Owner controls “undercut” profiles.

SETROPTS 14

```
COMPATIBILITY MODE IS NOT IN EFFECT
MULTI-LEVEL QUIET IS NOT IN EFFECT
MULTI-LEVEL STABLE IS NOT IN EFFECT
MULTI-LEVEL SECURE IS NOT IN EFFECT
MULTI-LEVEL ACTIVE IS NOT IN EFFECT
```

- MLS options:
  - Not generally used / only with caution

SETROPTS 15

```
CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT
USER-ID FOR JES NJEUSERID IS : ????????
USER-ID FOR JES UNDEFINEDUSER IS : ++++++++
```

- Catalogued data sets only (pre-SMS)
  - Requires use of special FACILITY class
    - ICHUNCAT
    - ???
- Define default userids for undefined work coming in from local JES and NJE.

SETROPTS 16

```
 PARTNER LU-VERIFICATION SESSIONKEY INTERVAL
MAXIMUM/DEFAULT IS 30 DAYS.
 APPLAUDIT IS NOT IN EFFECT
 PRIMARY LANGUAGE DEFAULT : ENU
 SECONDARY LANGUAGE DEFAULT : ENU
```

- APPC Verification – requires procedures for updating when passwords expire
- Track use of APPL profiles
- Primary / Secondary language support (aka NLS)

Critical RACF Services

RACF Subsystem

- It is NOT RACF!
  - Shutdown the subsystem has no impact on RACF
- Why have it?
  - Persistent APPC verification
  - RACF commands from console!
    - ?good or bad? -- It depends!

Installation

- Requires update to *parmlib*
  - Add IRRSSI00 definition to SCHEDxx
- Requires update to *proclib*
  - Add RACF procedure
- Requires a RACF parmlib
  - Ensure proper protection on data set
  - Review ALL members: IRROPTnn

RACF subsystem parmlib

- Do NOT use SYS1.PARMLIB
- Find in SYS1.PROCLIB(RACF)
- ANY command stored herein
  - Issued with SYSTEM SPECIAL authority.
  - No auditing is available
  - Contains RRSF network definitions

Shared System Considerations

- RRSF - RACF Remote Sharing Facility
  - Makes use of RACF address space
  - RRSFDATA class profiles
  - Set on user basis using RACLINK command
  - Key feature: AT(.userid) allows command to execute under other than current userid
  - Check for password sync
    - Useful for multiple userids / person
    - NOT for use by different users

R R S F

- Can be used both local (monoplex) or shared (sysplex)
- Local enables:
  - Synchronizing passwords on differing userids
  - Executing commands under different userids
  - Executing commands under same userid (in RACF address space)

USERID Audits

USER Audit

- **SPECIAL -** owns all profiles
- **OPERATIONS -** open any data set unless ACC(NONE)
- **AUDIT -** review controls, update LOGOPTIONS
- **REVOKE -** access removed
- **UAUDIT -** leave footprints EVERYWHERE
  good for short-term **–** but not for long term
- **PROTECTED –** CANNOT be used where passwords required
- **RESTRICTED –** No rule, no access

PROTECTED / RESTRICTED

- New in OS/390 2.8
  - PROTECTED
    - CANNOT be used wherever password validation occurs – every password specified is incorrect
    - CANNOT be REVOKEd for password violations
    - Set using ALU userid NOPASS NOOID

```
USER=SYSMSH2  NAME=MARK S. HAHN           OWNER=SEC
DEFAULT-GROUP=SYSPROG   PASSDATE=N/A      PASS-INTERVAL=N/A
  ATTRIBUTES=PROTECTED UAUDIT
```

PROTECTED / RESTRICTED

- New in OS/390 2.8
  - RESTRICTED
    - GLOBAL, UACC and ID(*) ignored
    - Must be given access
    - Useful wherever restricted access is required
    - Set using ALU userid RESTRICT

Lower Case userids?

- Introduced in 2.8
- NOT for installation use
- Non-standard userids: anchors for records in DIGTCERT and DIGTNMAP

```
COMMAND INPUT ===> tso sr class(user)
 irrcerta (user certificates with CERTAUTH)
 irrmulti (user certificates with SITE)
 irrsitec (certificate name filters)
...
```

- Breaks DSMON without toleration PTFs in shared RACF database at multiple levels
- Automatically created at IPL if not present at 2.8+

Utility Services

- IRRUT100
  - Data base search – some impact
- IRRUT200
  - Data base analyzer
  - Use with SYSUT1 (makes a copy)
  - Great for making a copy (low activity time)
- IRRUT400
  - Database reorg / split / merge utility

More Utility Services

- IRRDBU00
  - Data base unload – requires update access to database
  - Outputs text VB-format records for reporting
- IRRADU00
  - SMF reformatter
  - Exits within SMFDUMP
  - Functional support for new RACF records,
- IRRRID00
  - Remove ID utility
  - Reads IRRDBU00 output to build commands to remove userids and group ids (clean up)

I R R D B U 0 0

- User must have update access to database
- Run against recent *copy* of the database specifying NOLOCKINPUT
- Output is text and can be
  - Viewed directly
  - Input to installation programs
  - Manipulated via SORT/MERGE
  - Input to database management (DBMS e.g. DB2). Control statements included
- Record contents (layout) defined by “Record Type” 4-numeric digit field: ‘0110’ Group DFP Data; ‘0200’ User Basic Data,

I R R D B U 0 0

```
//jjj  JOB
//UNLOAD   EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT DD   SYSOUT=*
//DD1      DD   DSN=racf.database.copy,DISP=SHR
//OUTDD    DD   DSN=output.file,
//    dcb=(RECFM=VB,LRECL=4096)
```

IRRDBU00 output

```
IRR67010I Specified option: NOLOCKINPUT
IRR67013I Option in effect: NOLOCKINPUT
IRR67182I SYS3.RACF.BACKUP associated with DD INDD1 has been successfully
opened
IRR67007I The blocksize was taken from DD INDD1 and the data set was closed.
IRR67150I Processing 1 RACF data set(s).
IRR67182I SYS3.RACF.BACKUP associated with DD INDD1 has been successfully
opened
IRR67164I INDD1 is a backup data set. All input data sets must be backup
data se
IRR67093I Processing group profiles.
IRR67494I 172 group profile(s) have been unloaded.
IRR67093I Processing user profiles.
IRR67494I 1299 user profile(s) have been unloaded.
IRR67093I Processing dataset profiles.
IRR67494I 460 dataset profile(s) have been unloaded.
IRR67093I Processing general profiles.
IRR67494I 1 general RACFVARS profile(s) have been unloaded.
IRR67494I 1 general GLOBAL profile(s) have been unloaded.
IRR67494I 43 general FACILITY profile(s) have been unloaded.
IRR67494I 18 general UNIXMAP profile(s) have been unloaded.
IRR67402I Database unload utility has successfully finished processing.
```

I R R R I D 0 0

- Uses IRRDBU00 output as its input
- Other input is list of userids and group names to be removed from relevant fields in RACF database.
- DUMMY or null user list requests remove all references to non-existent ids.
- Output is TSO command stream – may require editing, especially *?id*

I R R I D 0 0

```
//jjj  JOB
//UNLOAD   EXEC PGM=IRRRID00
//SYSPRINT DD   SYSOUT=*
//SYSOUT   DD   SYSOUT=*
//SORTOUT  DD   work.file
//SYSUT1   DD   work.file
//INDD     DD   DSN=irrdbu00.output,disp=SHR
//OUTDD    DD   DSN=output.file,
//    dcb=(RECFM=VB,LRECL=259)
//SYSIN    DD   DUMMY  [find residual ids]
//SYSIN    DD   *
Oldid [replid]
```

IRRRID00 output

```
IRR68001I No IDs were found in the SYSIN data set. A search for all residual
   references
IRR68019I IRRRID00 has searched 10000 records and processed 0 records.
IRR68019I IRRRID00 has searched 14597 records and processed 0 records.
IRR68019I IRRRID00 has searched 14597 records and processed 14597 records.
IRR68004I IRRRID00 found 0 references.


PERMIT   MVS.*.STC.SYNRECAL  CLASS(OPERCMDS ) ID(SEC     ) DELETE
RALTER   OPERCMDS MVS.*.STC.SYNRECAL OWNER(SECURITY )
PERMIT   MVS.*.TCPIP.**  CLASS(OPERCMDS ) ID(SEC     ) DELETE
RALTER   OPERCMDS MVS.*.TCPIP.** OWNER(SECURITY )
```

R A C F I C E T O O L

- Found in SYS1.SAMPLIB(IRRICE)
- Uses SORT to produce reports from IRRDBU00 and IRRADU00 output

UGRP:Users With Extraordinary Group Authorities 99/04/13

User ID	Group	GrpSpec	GrpOper	GrpAudit
LCLAUDIT	GROUP1	NO	NO	YES
LCLOPER	GROUP1	NO	YES	NO
LCLSPEC	GROUP1	YES	NO	NO
UCAUDR$Y	GPCONNEC	NO	NO	YES
UCOPER$Y	GPCONNEC	NO	YES	NO
UCSPEC$Y	GPCONNEC	YES	NO	NO

Misc Concepts

UACC vs. ID(*)

- UACC = anyone(!) RACF defined or not
- ID(*) = anyone defined to RACF; not applicable to non-RACF defined users
- **Recommendation: wherever possible, replace UACC > NONE with UACC(NONE) and ID(*) ACC(uacc).**
- **Wherever “shared” userids, use RESTRICT**

System Entry

- Collect userid and password from requestor
  - TSO / CICS logon
  - JES job submission
  - APPC
  - MCS operator
- Additional checks
  - TSOPROC / ACCTNUM (resources)
  - SHIFT
  - APPL

System Entry control

- NODES class
- WRITER class
- APPL class
- TSO classes
  - ACCTNUM
  - TSOPROC
  - PERFGRP

A U D I T

- Level of access at which the access is to be recorded for both success and failures
- IF YOU AUDIT - REVIEW the logs!!
- AUDIT(FAILURES(READ)) strongly recommended.
- AUDIT(SUCCESS(UPDATE)) if you watch data set for most
- AUDIT(SUCCESS(READ)) for critical

Other Settings in Security Server

- NOADDCREATOR
  - Conditional default
  - Verify setting
  - Prevents exposure of old: creator on access list with ALTER

OMVS - OpenEdition MVS

- IBM reference page link
- OMVS = POSIX / UNIX on IBM mainframe
- OMVS segment in user and group profiles
  - UID(0) = SUPERUSER
  - GID(0) = nothing special
  - Nothing prevents multiple users / groups having same UID / GID - manual effort
  - Until R2.10, list Un and Gn for assigned userids
    - RLIST U0 UNIXMAP ALL
      lists all userids assigned to UID(0)

USER Audit - OMVS

- multiple fields in OMVS segment
  - User definition
    - UID(nn) - number (0 is superuser)
    - PATH(xx) - home directory
    - PROGrAM - shell
  - User limits (system limit overrides)
    - xxxMAX

Data Set / Resource Auditing

- Owner set audit levels
- Auditor set audit levels

UNIX Changes to RACF

- When UNIX System Services invoke RACF to make determination:
  - Pass UNIX FSP (File Security Packet)
  - RACF checks authorization: user, owning group or world and issues ICH408I and/or writes SMF record
  - RACF tracks userid AND uid – maintains individual accountability

Resource Class Auditing

- Ensure no IBM classes overridden
- Review definition for OPERATIONS
- Ensure naming standards for resource class names followed

RACF LISTxxxx Commands

- LISTUSER
  - Using Authorization groups details which services user authorized to
- LISTGROUP
  - Using authorization groups details who has access to the service
- LISTDSD
  - LISTDSNS – what cataloged data sets affected

- RLIST

The FACILITY Class

The FACILITY Class

- Define it
  - What is it?
  - Why use it?
  - Who uses it?
  - How is it used?
  - Where is it used?

What is the FACILITY class?

- RACF class
- Known characteristics from CDT:
  - 39 characters maximum
  - GENERIC supported
  - RACLIST? Probably / *should* be
  - UACC(NONE)
  - OPERATIONS not honored

Why use FACILITY?

- It’s already there: Present in every system
- No need to define a new class
- It’s a recommendation – resource manager decides to honor

Who uses FACILITY?

- Any *authorized* application
- List of applications always changing – NO central registry – OYO!
- IBM
  - Dynamic Contents Supervisor
  - SecureWay Security Server (RACF)
  - UNIX System Services
- OEM
  - Most often security interfaces

How is FACILITY used?

- Authorization checking
  - "Is user allowed to access this resource?"
- Processing switch
  - Presence of profile changes internal processing (e.g. RJE and NJE)
- Default storage
  - Easily retrieved widely-used information (e.g. BPX.DEFAULT.USERID)

What FACILITY Profiles Already Exist?

- SR CLASS(FACILTY) [NOMASK | MASK(bpx.*)]

```
BPX.DAEMON
BPX.DEFAULT.USER
BPX.SMF
BPX.SUPERUSER
```

- IRRDBU00

```
----+----1----+----2----+--

0505 BPX.DAEMON
0505 BPX.DAEMON
0500 BPX.DAEMON
0500 BPX.DEFAULT.USER
```

```
sssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssssss
s
.IRRDBU00.DATA                          Line 00013881 Col 233 312
                                                Scroll ===> CSR
5----+----6----+----7----+----8----+----9----+----0----+----1-
-
   GLOBAL   NO   017 1998-12-04 SYSPROG  1998-12-04 1998-12-04
   FACILITY SEC      READ     00000
   FACILITY STARTED  READ     00000
   FACILITY YES  019 1999-01-18 SEC      1999-01-18 1999-01-18
```

Characteristics

- AUDIT(ALL(SUCCESS)) to see which are used when
- RACF passive: only referenced if interface calls
  …
- Some IBM resource managers write SMF records – usually SMF090-xx
- Others may write user SMF records
- Either: READ = yes, NONE = no
  -or- UPDATE=change, READ=audit, NONE=no
  Defined by the application; no hard rule

Gotcha's

- Do NOT backstop at base level: ** or *.* *This will return "profile defined" which may activate services based upon a profile be defined (e.g. a switch profile: NJE.** and RJE.**)*
- Cannot sub-delegate (CLAUTH) class authority; perhaps GENERICOWNER, but see above.

Alphabet Soup

- **ADM.ADMPQM** control GDDM Print Queue Facility
- **ADR.**** DSS
- **ARC.**** HSM
- **BPX.**** UNIX System Services
- **CBD.CPC.dataset** Hardware Configure Defn (HCD)
- **CDS.CSSM.**** Open Cryptographic Services
- **CSR.BLSRHIPR.ssnm** control Local Shared Resource
- **CSV*.**** OS/390 Dynamic contents
- **EDG.**** RMM
- **ERBSDS.*** RMF access to SMF data for sysplex
- **IDC.**** ICFCAT
- **IGG.**** Catalog

Alphabet Soup

- **IGD.**** DFP
- **IHJ.CHKPT.volser** define checkpoints on shared DASD
- **IHV.function** ESCON device controls
- **IOA.*** OSA/SF Open System Adapter
- **IRR.**** SecureWay Security Server
- **MVSADMIN.**** Sysplex management
  including coupling facility, logstreams and other residents
- **NJE.nodename** Network Job Entry (switch)
  profile found to match node, RACF password controls active
- **RJE.linename** Remote Job Entry (switch)
  profile found to match terminal_id, RACF password controls active

Alphabet Soup (3)

- **STGADMIN.**** Data Management
- But wait … there's even *still* more!

Miscellaneous

- **APPCMVS.** –** APPC/MVS controls
- **ATBTRACE.netid.lu-name.tp-name –** Start/stop API traces
- **DITTO.function.function –** MVS/Ditto
- **FWKERN.** -** Firewall kernel authorization
- **IMSXCF.name1.name2 –** MQSeries connecting to IMS users
- **PSP.ASFPPIPE.subsys –** batch pipe
- **TPI.IMSSOCK.trancode –** IMS use of IP sockets

And more with every new release of OS/390 and z/OS (66 web hits for FACILITY class in R2.10).

Remember, these are just the IBM-defined; there are multiple OEMs also

Dynamic Contents

What resources are defined herein?

- **CSVDYNL.** –** Dynamic Link list
- **CSVLLA.** –** Link Library Lookaside
- **CSVDYLPA.** –** Dynamic LPA
- **CSVAPF.** --** Dynamic APF
- **CSVDYNEX.** -** Dynamic Exits
- **CSVRTLS.LIBRARY.library.version –** Run Time Lib Serv

Review PROGxx writeup for greater specifics

Must use Content service commands, macro calls, etc.

IRR.** RACF-Related

- Frequently unscoped (all or none)
- **IRR.LISTUSER** – enables non-SPECIAL users to list base segments of user profiles
- **IRR.RESET.PASSWORD** – enables non-SPECIAL users to reset passwords for un-privileged users
  - READ allows RESUME and change to expired password
  - UPDATE allows NOEXPIRED password
  - New in 2.4 w/retrofit to 2.3 via PTF

More RACF Uses

- **IRRDPI00** – STC for IRRDPTAB must have READ
- If SETROPTS NOCATDSN in effect:
  - **ICHUNCAT.dataset.name** w/READ
  - **ICHUSERCAT –** READ allows STEPCAT or JOBCAT usage

Still More RACF Uses

- **IRR.DIGTCERT.func** – Digital Certificates
- **IRR.RDCERUID** – SAF Callable Service: R_dceruid (maps DCE UIDs to RACF userid)
- **IRR.RTICKETSERV** – R_ticketserv service
- **IRR.RUSERMAP** – R_usermap service
- **IRR.RADMIN.cmdname** – execute RACF TSO command using R_Admin.
- **IRR.RPKISERV.func** – retrieve v.509 certificates

UNIX System Services

- BIG user!
  - Discussed greater depth in UNIX System Services Audit
- Define UNIX uids; either
  - unique UNIX uids or
  - default UID/GID for “generic” UNIX users: FTP BPX.DEFAULT.USER
  - Control use of many (most?) services:
    - Superuser
    - Daemons / servers
    - Enhance UNIX standard security

BPX.** profiles

- **BPX.DAEMON** – restricts access to daemon services
- **BPX.DEBUG** – restricts access to ptrace (via dbx) for debugging APF or server authority programs
- **BPX.FILEATTR.APF** – Authorizes users to set the APF attribute on HFS files. Similar to update access to SYS1.LINKLIB or SYS1.LPALIB
- **BPX.FILEATTR.PROGCTL** – controls setting program-controlled attribute … allows execution with high level of authority
- **BPX.FILEATTR.SHARELIB** – controls use of shared library region
- **BPX.JOBNAME** – who can set their own jobnames using _BPX_JOBNAME . (READ or higher)
- **BPX.SAFFASTPATH-** see separate foil
- **BPX.SERVER** – allows create/delete security environment for caller's thread; also determines authorization to access OS/390 resource

BPX.** profiles (2)

- **BPX.SMF** – whether a user may cut SMF records
- **BPX.STOR.SWAP** – which users may mark address spaces non-swappable
- **BPX.SUPERUSER** – make use of switch user (*su*) command
- **BPX.WLMSERVER** – controls access to WLM server functions

BPX.SAFFASTPATH

- Successful security checks are not audited. *If you need to audit successful security checks, do not define this profile.*
- Activated either by IPL or by SET OMVS= **after** profile defined.
- If using IRRSXT00 exit to control HFS access, DO NOT use this profile.
- Auditing successful HFS accesses is a LOT of records.
- New in R2.10 found in RACF-L; SMF type 80 for FSOBJ.

Discrete Resources

- **AOPADMIN –** Infoprint server ISPF panels (JAVA)
- **CSFTTKE –** TKE Host Transaction Program
- **IEAVECTOR –** access to vector processes
- **IEAABD.DUMPAUTH –** controls address space dumps (READ=must have program control access; UPDATE=no need to satisfy program controls)
- Tape
  - **IEC.TAPERING**
  - **ICHBLP** (Bypass Label Processing)*
  - **ICHNL** (No Label Processing)*

* requires TAPEVOL class active

Special Function Profiles

- These set switches / store defaults, no access list
  - **BPX.DEFAULT.USER**
  - **BPX.SAFFASTPATH**
  - **NJE.nodename**
  - **RJE.linename**

Resources

- How to find more about FACILITY?
  - Scan the web: www.s390.com/os390, http://redbooks.ibm.com
  - Search the CD-ROM
  - Read publications: NaSPA Technical Support magazine
  - GARUG listed resources
  - RACF-L questions

Summary

- Every Security Server installation has FACILITY available for use – no system modifications required as with installation defined class.
- Characteristics well documented: 39-char limit, RACLISTed, does not honor OPERATIONS
- 3 types of profiles: authorization, switch set, default storage
- OEMs may not invoke requisite system services to enforce expected authorizations

S u m m a r y

- DO NOT backstop at top level: *.* or **
- No central registry of profiles, IBM or OEM
  Use ‘SR CLASS(FACILITY) NOMASK’ to see all or to build RLIST CLIST for execution

S U M M A R Y

Resources and Tools

- RACF-L listserv group
- RACF CD-ROM
- RACF web page
- OS/390 web page
- OS/390 R3 announcement letter

Glossary

- PADS - Program Access to Data Sets , a.k.a. Program pathing

Abstract

- More and more OS/390 services are turning to RACF to help secure them; so we're very lucky, aren't we? Does the proliferation of services make our job easier or more challenging? This 1/2-day workshop will explore the basic RACF settings of old and examines those new settings being introduced twice yearly in every new release of the operating system. Instead of playing catch up, learn what is coming in the announced releases so that you can be ready when asked about a new service. For example, when TCP/IP is installed, what changes to the LINKLST, LPALST, SCHEDxx, IKJTSO00 services are expected and normal? Can you use RACFICE to report on RACF settings, SMF records, etc? Is DSMON still a valuable audit tool? Should RRSF be used in a monoplex? Are the SMF090 records keeping pace with the changing system environment? These and other perplexing questions are answered in this workshop.