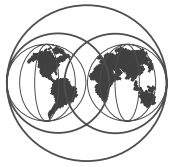


RACF Facilities for Everyone!

Mark Nelson
System/390
IBM Corporation
Department BWVA Mail Station P385
Poughkeepsie, NY 12601

RACF- 99
Session 29
June, 1999

Phone: (914) 435-7758
Internet: markan@us.ibm.com
IBMMAIL: USIBMV4B@IBMMAIL

Agenda

- **RACF 2.1**
  - Dynamic Started Procedures Table
  - SMF Data Unload Utility
  - RACROUTE REQUEST=LIST,GLOBAL=YES
- **RACF 2.2**
  - Program Control Enhancement
  - Remove ID Utility
  - Enhanced PassTickets
  - Unloading SETROPTS and RVARY with IRRADU00
  - Remote Sharing Facility
  - Year 2000
- **OS/390 Release 3 Security Server**
  - Command Exit
  - Prevent Automatic Addition of Creator
  - Controlling Program Access by SMF System ID
  - Password Reset Only

Agenda...

- **OS/390 Release 4 Security Server**
  - RACF Control of DB2 Objects
  - Password History Enhancement
  - Default UID and GID for OpenEdition
  - Support for Digital Certificates
- **OS/390 Release 6 Security Server**
  - Networked Qualified Names
  - Digital Certificate Enhancements
- **OS/390 Release 8 Security Server**
  - Protected User IDs
  - UNIX System Services SuperUser Granularity

RACF 2.1

Started Procedures Table - Before

- What is a started procedure table - ICHRIN03
- Assembled and linked into LPA
- Problems:
  - Requires an IPL to change
  - Strict format requirements
  - Must run DSMON to see what is in use

SYS1.LPALIB(ICHRIN03)

```
ICHRIN03 CSECT
         Title 'ICHRIN03'
         DC XL2'800B'
         *--------------------
         DC CL8'JES2    '
         DC CL8 'JES2    '
         DC CL8 'STCGRP  '
         DC XL1 '40'
         DC XL7 '00'
         *--------------------
         DC CL8'CICS    '
         DC CL8 'CicsProd'
         DC XL1 '80'
         DC CL8 'STCGRP  '
         DC XL7 '00'
         *--------------------
```


Dynamic Started Procedures Table

- Advantages:
  - Ability to use STARTED class or ICHRIN03
  - Easier to define
  - Allows changes to security definitions for stared tasks without an IPL
  - Supports MVS 5.1 START command enhancements
  - Better generic support that ICHRIN03
  - Easier to see what is being used

A new class - STARTED

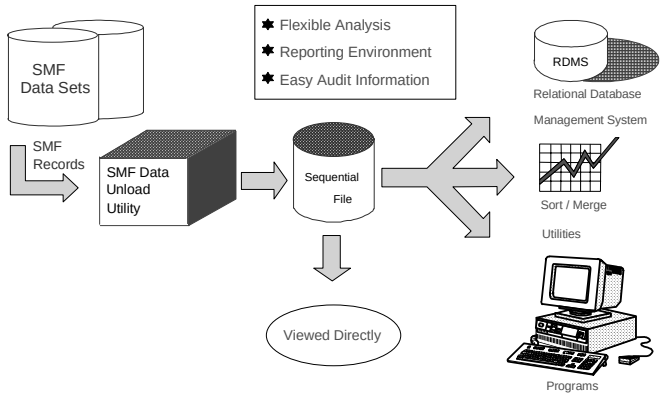
```
RDEFINE STARTED JES2.* STDATA(USER(JES2)
        GROUP(STCGRP) TRUSTED(YES))
RDEFINE STARTED ** STDATA(USER(=MEMBER)
        GROUP(STCGRP) TRACE(YES))
SETROPTS CLASSACT(STARTED) RACLIST(STARTED)
```

JES2.*	User ID	Group ID	Flags
CICS.PROD*	.....		

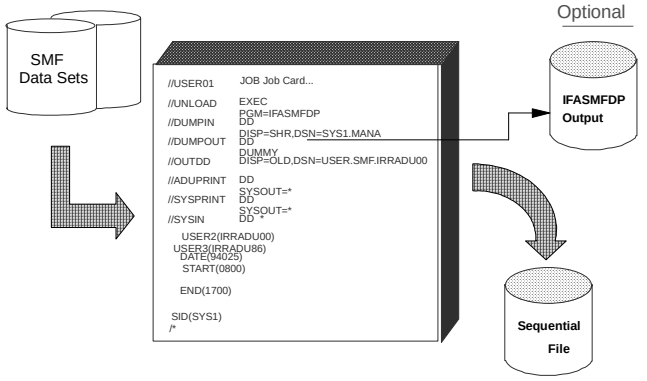
Dynamic Started Procedures Table - Migration

- **SYS1.SAMPLIB Support:**
  - New member ICHSPTCV - REXX exec to convert ICHRIN03 entries
- **New Messages:**
  - IRR812I - issued when STARTED class profile used (TRACE=YES)
  - IRR813I - issued when STARTED class profile not found
  - IRR814I - issued when STARTED class profile incomplete
- **Works on any MVS release supported by RACF 2.1**
- **Must keep ICHRIN03!**

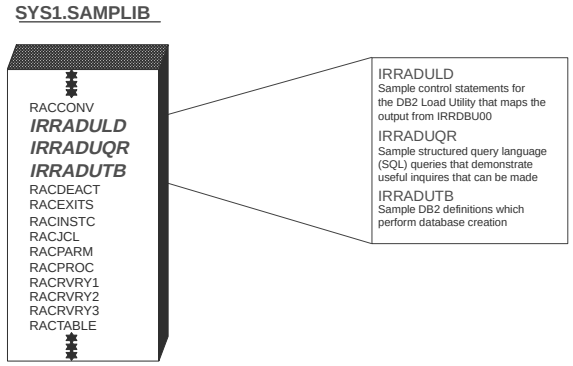
RACF SMF Data Unload Utility



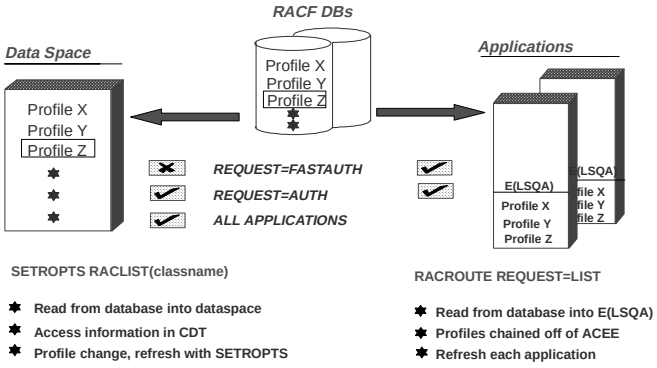
How is the Utility invoked ?



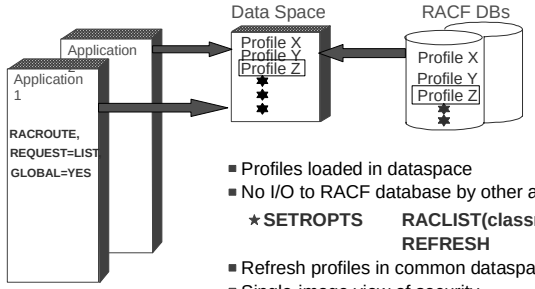
Sample DB2 Mappings



RACLIST PROCESSING (PRE 2.1)



RACROUTE REQUEST=LIST,GLOBAL=YES



- Profiles loaded in dataspace
- No I/O to RACF database by other applications
  - ★**SETROPTS RACLIST(classname) REFRESH**
- Refresh profiles in common dataspace
- Single-image view of security
- Refresh propagated to members in sysplex
- Better use of real storage

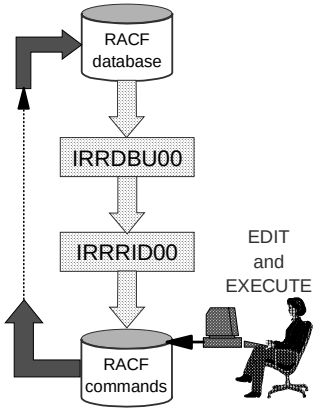
RACF 2.2

Program Class Enhancement

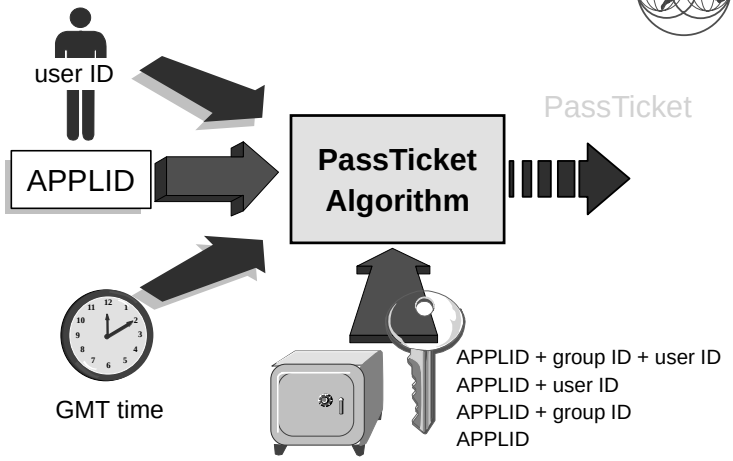
- **Volume specification for program definitions is now optional!**
  - OLD: `RDEFINE PROGRAM xxx ADDMEM('library'/volser)`
  - NEW: `RDEFINE PROGRAM xxx ADDMEM('library')`
- **Shipped with APAR OW24881**
  - PTF UW36135 for RACF 2.2, OS/390 Security Server Release 1 and OS/390 Security Server Release 2
  - PTF UW36136 for OS/390 Security Server Release 3

RACF Remove ID Utility

- **Creates RACF commands that assist in housekeeping**
- **Output must be reviewed and edited**
- **Can be used to remove any reference to residual IDs**
- **Removes deleted user IDs and group IDs from access lists**
- **Replaces user IDs and group IDs in owner fields**



Qualified PassTicket Profile



RACF Remote Sharing Facility

- **Links multiple RACF DBs, providing:**
  - Command direction
  - Password synchronization
  - Automatic command direction
  - Automatic password direction
- **Benefits of using with one RACF DB:**
  - Execute commands under different ID
  - Password sync on single system
  - RACF commands from the operator's console

Unloading SETROPTS and RVARY

- **IRRADU00 now unloads the keywords that were specified on SETROPTS and RVARY**
- **When more than 10 classes are specified on a keyword, such as "CLASSACT(class1, class2...)", the first 10 classes are unloaded, along with a count of the classes not unloaded**
- **Specifying "*" for a class list yields a "*" in IRRADU00 output**
- **New field in SETROPTS SMF type 6 relocate section to indicate that "*" was specified .**
- **Support delivered via APAR OW30252, for RACF 2.2 and all OS/390 releases**

Year 2000

- **RACF is Year 2000 compliant with APAR OW19521**
  - RACF has many dates in the RACF database that are three character packed decimal values, of the form yydddf, where "yy" represents the year.
  - Dates with a "yy" value of "70" or earlier are considered to be in the year 20yy. Dates with a "yy" greater than 70 are considered to be in the year 19yy.
- **APAR OW19251**

OS/390 Security Server Release 3

Prevent Automatic Addition of User ID to Access List

- **New SETROPTS option to control the placement of the profile creator on the access list**
  - ADDCREATOR - Adds the creator (business as usual)
  - NOADDCREATOR - Do not add the creator
    - Any profile created by ADDSD or RDEFINE
    - Any generic profile created by RACROUTE REQUEST=DEFINE
    - Discrete profiles *excluding* DATASET and TAPEVOL

RACF Command Exit

- **New exit point IRREVX01 invoked for each end-user RACF command (operator commands, RVARY, and BLKUPD excluded)**
- **Uses MVS Dynamic Exit Services**
  - Exit can be replaced without an IPL
  - Exit can have an installation-chosen name
  - Multiple modules can be associated with a single exit point
- **Exit may fail the command with or without a message**

Controlling Program Access by SYSID

- **Access to programs (load modules) can now be controlled based on SMF system ID**
- **New WHEN option:**
  - PERMIT *progname* CLASS(PROGRAM) ID(MARKN) WHEN(SYSID(*smf_system_id*))
- **WHEN(SYSID(....) valid only for PROGRAM profiles**
- **No class associated with the SYSID**
- **SYSID value not verified**
- **Support delivered via APAR OW25727, PTFs UW91104 for R3, and UW91105 for R4**

Password Reset Only

- **Users may now be authorized to reset passwords, resume user IDs, and list profiles for others without being given SPECIAL or group-SPECIAL authority.**
- **Controlled by FACILITY Class Profiles :**
  - **IRR.PASSWORD.RESET**
    - **READ** Access - Reset password to expired value and ability to resume a user.
    - **UPDATE** Access - May reset password to a non-expired value and resume a user
  - **IRR.LISTUSER**
    - **READ** Access - May list other user's profiles via LISTUSER, subject to field-level access checks
- **Available on R3 in support of TIVOLI Roles Based Administration Enhancements.**

User Administration Enhancements

- **Prior to release 6, a user's password was set to an expired temporary password value when the password was changed by an administrator.**
- **Now, there is a new option (NOEXPIRED) on ALTUSER which allows the setting of a password which does not have to be changed on first use.**
- **Available with APAR OW26060 on R3 and R4.**

OS/390 Security Server Release 4

RACF Control of DB2 Objects

- **DB2 - Access Control Authorization Exit Point**
  - A new exit point documented by DB2
  - Exit point is driven:
    - Once at subsystem startup
    - For each DB2 authorization request
    - Once at subsystem Termination
  - DB2 Provides dummy DSNX@XAC routine
- **RACF - The RACF/DB2 External Security Module**
  - Fully supported exit module designed to receive control from the DB2 Access Control Authorization Exit Point
  - Translates DB2 authorization checks into checks in RACF general resource classes

Password History Enhancement

- **Pre-release 4, a user's current password was not placed in the password history when the password was changed by an administrator.**
- **With release 4, the user's current password is placed in the password history when the password is changed by an administrator.**
- **Helps prevent users from circumventing password change frequency rules by calling up the help desk and having the administrator reset their password to a temp value, which they can change back to their favorite value that they had been using.**

Default UID/GID

- **Pre-release 4, all UNIX System Services users must:**
  - Have a valid UID
  - Be connected to at least one group with a valid GID
- **With release 4, installations can:**
  - Assign users without a UID/GID an installation defined UID/GID
  - Assigned through a FACILITY class profile:
    - BPX.DEFAULT.USER APPLDATA('*userid/groupid*'), where *userid* and *groupid* are the RACF user ID and group ID that are to be assigned.
    - Access list and UACC are not used
- **Benefits:**
  - Ease of administration without loss of audit trail

RACF Support for Digital Certificates

- **With OS/390 Security Server R4, RACF can be used to map certificates to a RACF user ID.**
  - New general resource class (DIGTCERT)
    - New segment (CERTDATA) contains the certificate
    - APPLDATA contains the user associated with the certificate
    - UACC contains the TRUST status of the certificate
    - New user profile repeat group points to the certificate
  - New RACF command (RACDCERT) to manage the certificates

RACDCERT Command Syntax

```
RACDCERT
   [  ID(UserID) ]
   [  LIST
    | ADD('Dataset-Name')
          [ TRUST | NOTRUST ]
    | ALTER [ (SERIALNUMBER(Serial-Number)
                [ ISSUERSDN('Issuer's Distinguished
                                Name') ] ) ]
              TRUST | NOTRUST
    | DELETE [ (SERIALNUMBER(Serial-Number)
                [ ISSUERSDN('Issuer's Distinguished
                                Name') ] ) ]
   }
```


How are Certificates Used?

- **initACEE callable service is enhanced to allow the specification of a certificate**
- **RACF verifies that the certificate is:**
  - Registered with RACF
  - Trusted
  - Maps to a valid user ID
- **initACEE returns the security environment for the user to which the certificate is associated**
- **Used by the Lotus Go Domino Webserver for OS/390 (formerly the Internet Connection Secure Server)**

OS/390 Security Server Release 5

New Certificate Support in V2R5

- Certificate Autoregistration
- RACLISTing DIGTCERT optional
- New Base64 certificate format
- CICS certificate to user ID translation
- Additional functions/keywords on RACDCERT to associate a label with a certificate
- OS/390 V2R5 APARs
  - RACF (R4) - OW31933
  - SAF OW31934
  - OpenEdition - OW33091
  - LE (C-RTL) - PQ15716

New RACDCERT Command Syntax

```
RACDCERT
   [  ID(UserID) ]
   [  LIST   [(LABEL('label-name') | [
               SERIALNUMBER(Serial-Number)
               [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ]
    | ADD('Dataset-Name')
         [ TRUST | NOTRUST ]
         [WITHLABEL('label-name')]
    | CHECKCERT('data-set-name')
    | ALTER [(LABEL('label-name') | [
               SERIALNUMBER(Serial-Number)
               [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ]
              [TRUST | NOTRUST]
    | DELETE [(LABEL('label-name') |
                [ (SERIALNUMBER(Serial-Number)
                [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ]
```


OS/390 Security Server Release 6

User Administration Enhancements

- Prior to release 6, a user's password was set to an expired temporary password value when the password was changed by an administrator.
- Now, there is a new option (NOEXPIRED) on ALTUSER which allows the setting of a password which does not have to be changed on first use.
- Available with APAR OW26060 on R3 and R4.

NQN - Network Qualified Names

- Ability to specify an additional qualifier in APPC information passed to RACF to identify the remote network in existing APPCLU, APPCPORT classes.
- Allows customers with interconnected networks containing like named LU's to differentiate them.
- Changes you'll see :
  - New Keyword POENET on RACROUTE
  - APPCPORT class expanded from 8 - 17 chars using new MAXLENX parameter on ICHERCDE macro
  - DISPLAY, PERMIT and TARGET commands accept 17 char partner-LU name
  - Panels, SMF Unload and DB Unload will support new extended name length.

OS/390 Security Server Release 8

Protected User ID

- User ID which has no password and may not be logged on
- Key uses:
  - Started tasks
  - UNIX daemons
  - Subsystem resource managers
- Prevents revocation due to excessive password attempts
- Implemented by specifying "NOPASSWORD" and "NOOIDCARD" on the ADDUSER and ALTUSER command
- IRRDBU00 field USBD_NOPWD new value: "PRO"

SuperUser Granularity

- Authorize selected users to do selected SuperUser functions without giving UID 0 or access to BPX.SUPERUSER profile
- New UNIXPRIV class to define resources
- Example: give user LAURIE the authority to mount and unmount any file system:

```
RDEFINE UNIXPRIV SUPERUSER.FILESYS.MOUNT UACC(NONE)
PERMIT SUPERUSER.FILESYS.MOUNT CLASS(UNIXPRIV)
  ID(LAURIE) ACCESS(UPDATE)
SETROPTS CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
```

- Some other things you can use this for:
  - Allow a user to read or write to any HFS file
  - Allow a user to send signals to any process
  - Allow a user to view all processes
  - Allow all users to issue chown for their own files

User Limits

- Allow selected users to exceed resource limits in the BPXPRMxx member of PARMLIB without giving UID 0
- New fields in the OMVS segment of the user profile to define resource limits
- Example: Give user UNIXUSR the ability to use more CPU time than the maximum specified by the MAXCPUTIME parameter of BPXPRMxx

```
ALTUSER UNIXUSR OMVS(CPUTIMEMAX(5000))
```

- Some other things you can use this for:
  - Set maximum address space size
  - Set maximum number of files per process
  - Set maximum number of processes per UID
  - Set maximum number of threads per process
  - Set maximum memory map size

Reminder: Service End Dates

- **RACF 1.9.0 and RACF 1.9.2**
  - Ended on 26 April, 1997
  - Announcement Letter 996-076 contains the details
- **RACF 2.1**
  - Ends on 06/30/99
  - Announcement letter 997-230 contains the details

RACF Home Page

- **http://www.s390.ibm.com/racf**
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - DBSYNC to compare/sync. two RACF data bases
    - RACFICE to create audit/analysis reports
    - OS390ART for a web-based reporting tool
    - RACTRACE tracing facility
    - RACFDB2 conversion utility
  - Frequently asked questions
  - RACF user group information