z/OS V2.5 IBM Education Assistant

Solution Name: Encrypt the RACF® Database Statement of Direction: *Technology Preview*

Solution Element(s): RACF

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Objectives: The Real Agenda

- Review the RACF V2R5 Statement of Direction for RACF database encryption
- Explain the configuration considerations
- Describe the V2R5 GA Supported Configuration
- Describe the changes with a RACF VSAM data set
- Describe the Installation, Exploitation and Coexistence
- Explain the planned documentation changes

Overview: The RACF V2R5 Statement of Direction

- Who does this statement of direction affect? z/OS:
  - System security architects
  - System auditor
  - z/OS auditors
  - z/OS system programmers

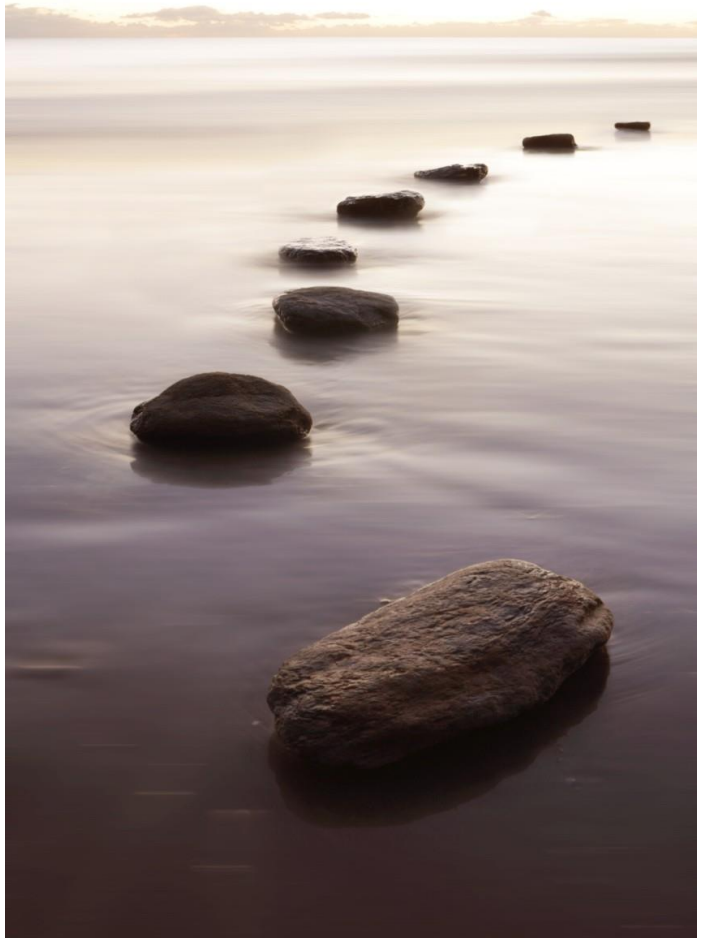
- What/Wow (Solution/Benefit/Value, Need Addressed)

  - "IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations."

Statement of Direction…

“IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations.”

- Full support will not be the in initial delivery of z/OS V2R5. Support may be delivered in a future release or as continuous delivery on V2R5.



Statement of Direction…

"IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations."

- "VSAM": Currently, RACF is its own access method. Leveraging the existing access control mechanisms for pervasive encryption means moving to an access method which supports encryption.

- Key reasons for the selection of a VSAM linear data set:
  - Consistency with existing RACF data access mechanisms
  - Consistency with existing RACF serialization mechanisms
  - Ability to utilize existing VSAM diagnostics
  - Ability to rely more on standard z/OS skills
  - Ability to leverage additional I/O infrastructure improvements in the future.

Statement of Direction…

“IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations.”

- “encrypted”: With RACF as its own access method if RACF were to perform its own encryption, RACF would be required add encryption calls to all of the places where RACF performs I/O (the RACF data manager, many of the RACF utilities). We are planning on leveraging VSAM’s pervasive encryption facilities.

Statement of Direction…

"IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations."

- "specific configurations": There are many things which need to be considered when discussing RACF's different configurations
  - How the RACF base is shared with other systems
  - How the system serialization performed across of the systems sharing the RACF data base
  - How the critical system objects (RACF data sets, catalogs) shared with other systems
  - How RACF is configured (sysplex communications, data sharing mode, etc.)

Configuration Considerations

- RACF is critically dependent on serialization:
  - RESERVEs on the volume which contains a RACF data set
  - ENQs
    - Some are SYSTEMS, some are SYSTEM, some are TASK
  - RACF's serialization actions depend on the RACF configuration
    - RACF data set location (shared vs. non-shared UCB)
    - Enablement of RACF's data sharing or falling back into READONLY mode
- Specific configurations will be announced as our testing of different environments progresses

The V2R5 GA Supported Configuration

- At GA of V2R5, RACF supports VSAM RACF data set that is:
  - Non-shared (may be on a device marked as shared)
  - Single RACF data set
    - That is, the RACF data base may not be split into multiple data sets
    - May have both a primary and a backup RACF data setback
  - Running in application identity mapping (AIM stage 3)
  - That is free from internal errors (IRRUT200 and IRRDBU00 run without error)
  - Non-SMS managed
  - Not in RACF sysplex communications mode or RACF data sharing mode
  - In a non-production and non-quality assurance (QA) environment

Changes with a RACF VSAM Data Set

- No change to the RACF programming interfaces (RACROUTE, ICHEINTY, RACF Callable Services, IRRXUTIL, RACF commands)

- No changes to the RACF serialization structure (major names of SYSZRACF, SYSZRACn)
    - But there is a new SYSVSAM ENQ.

- Applications which read the RACF data base directly *may* have actions to take to support VSAM

    - Disclosed at the vendor disclosure meeting in April 2020 and September 2020 and through ICN 1775 (18 August, 2020)

Usage and Invocation

RACF Utilities

- At GA of V2R5, the RACF utilities which are planned to support a RACF VSAM data set are:
  - IRRMIN00: RACF Database Initialization Utility
  - IRRUT100: RACF Cross Reference Utility
  - IRRUT200: RACF Copy and Index Validation Utility
  - IRRUT300 (BLKUPD): RACF Database Update Utility
  - IRRUT400: RACF Split/Merge Utility
  - IRRDBU00: RACF Database Unload Utility
- The utilities which do not process a RACF data set and are not affected by the use of a RACF VSAM data set are:
  - IRRDPI00: RACF Dynamic Parse Utility
  - IRRBRW00: RACF RRSF VSAM Data Set Browse Utility
  - IRRRID00: RACF Remove ID Utility
  - IRRADU00: RACF SMF Unload Utility
- The utility which will not support a RACF VSAM data set is:
  - IRRIRA00: RACF Internal Reorganization of Aliases

Dependencies/Installation

Dependencies (for the V2R5 technology preview)

- There are no software dependencies
- There are no hardware dependencies
- There are no exploiters

Installation

- There are no actions that need to be taken during the installation of z/OS V2R5 or upon the first IPL of z/OS V2R5

Upgrade and Coexistence Considerations

Coexistence

- All systems sharing a RACF VSAM data set must be running z/OS V2R5.
- A RACF VSAM data set may not be shared across systems until further support is announced

Exploitation

- This function is enabled only when a VSAM data set is introduced as a primary or backup RACF data set.
- A RACF VSAM data set can be introduced either at the time of IPL or by RVARY processing
- IRRUT200 introduces a new parameter, **`PARM=RENAMEACTIVATE(`*`dsn`*`)`**, which:
  - Copies the RACF data set to DDNAME SYSUT1
  - Renames the current inactive RACF backup data set to the name specified in the RENAMEACTIVE keyword (*dsn*)
  - Renames the SYSUT1 data set to the inactive RACF backup data set name
  - Activates the inactive RACF backup data set

Exploitation: VSAM Data Set Requirements

- A RACF VSAM data set must be allocated:
  - As a non-encrypted data set*
  - As a VSAM LINEAR data set*
  - With SHAREOPTS(3 3)*
  - With a CISIZE of 4096*
  - With the REUSE attribute*
  - With zero secondary cylinders
  - With zero free space
  - On a single volume

  (*) = Validated by RACF during IPL, RVARY ACTIVE, and IRRUT200 PARM=ACTIVATE|RENAMEACTIVATE

- A RACF VSAM data set can be introduced either at the time of IPL, RVARY ACTIVE, or IRRUT200 PARM=ACTIVATE|RENAMEACTIVATE

Exploitation: Creating a RACF VSAM Data Set

- The IDCAMS DEFINE CLUSTER statement to allocate a RACF VSAM data set is:

```
DEFINE CLUSTER (NAME('SYS1.RACFBACK.VSAM')  -
 LINEAR                                     -
 NONSPANNED                                 -
 ERASE                                      -
 REUSE                                      -
 SHAREOPTIONS(3,3)                          -
 VOLUMES(volser))                           -
 DATA(                                      -
    NAME('SYS1.RACFBACK.DATA')              -
    CISZ(4096)                              -
    CYLINDERS(num 0)                        -
    FREESPACE(0 0)                          -
    )
```

- Note the use of the DATA sub-keyword to explicitly allocate the name of the VSAM data component instead of accepting the default of "*dsn*.DATA"
- This newly created VSAM data set must be the target of the IRRMIN00, IRRUT200, or IRRUT400 utilities before it is used as a RACF VSAM data set.

Exploitation: IRRMIN00

- Initializing or updating the templates on a RACF VSAM data set with IRRMIN00 is done the same was as for a non-VSAM data set:

```
//IRRUT404 EXEC PGM=IRRMIN00,PARM=UPDATE
//SYSRACF  DD  DISP=SHR,DSN=RACFDRVR.MARKN.VSAM.TEST
//SYSPRINT DD  SYSOUT=*
```

Exploitation: IRRUT400

- Initializing a RACF VSAM data set with IRRUT400 (RACF Split/Merge/Reorg utility) is done the same was as for a non-VSAM data set:

```
//IRRUT400 JOB Job Card…
//IRRUT400 EXEC PGM=IRRUT400,PARM='NOLOCKINPUT'
//SYSPRINT DD  SYSOUT=*
//INDD1    DD  DISP=SHR,DSN=RACFDRVR.MARKN.VSAM04
//OUTDD1   DD  DISP=SHR,DSN=RACFDRVR.MARKN.VSAM.TEST
```

- Reminder: Split data sets are not allowed on input or output

Exploitation: IRRUT200

- The IRRUT200 (copy/index validation utility) is updated with a new PARM= value, PARM=RENAMEACTIVATE(dsn), which causes IRRUT200 to:

  1. Copy an existing RACF data set from SYSRACF to the SYSUT1 (the output data set)
  2. Rename the existing and inactive RACF backup data set to the value specified in RENAMEACTIVATE ("dsn" in this example) ***to get it out of the way***
  3. Rename the output data set to the inactive RACF backup data set name
     - If the output data set is VSAM, only the cluster is renamed
  4. Activate the backup RACF data set

- If IRRUT200 encounters an issue, it renames data sets back to their original state and leaves the backup inactive

```
//IRRUT200 JOB Job Card…
//IRRUT200 EXEC PGM=IRRUT200,PARM='RENAMEACTIVATE(SYS1.RACFBACK.O)'
//SYSRACF  DD  DISP=SHR,DSN=SYS1.RACFBKUP
//SYSUT1   DD  DISP=SHR,DSN=SYS1.RACFBKUP.VSAM
//SYSUT2   DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  DUMMY           Ignored for PARM=RENAMEACTIVATE
```

Exploitation: IRRUT200…

- Renaming the cluster name may obfuscate the relationship between the cluster name and the data component
  - VSAM displays the relationship in a LISTCAT ENTRY(dsn) ALL
  - Only the cluster name is used for authorization checking

- Assigning the data component a name that is your current back-up data set name appended with “.DATA” make the relationship clear, without having to do a LISTCAT ENTRY(dsn) ALL.

Exploitation: IRRUT200…

- Note that **`PARM=RENAMEACTIVATE(`*`dsn`*`)`** *may* cause a different profile to protect the backup RACF data set.
  - If your existing RACF backup data set is protected by a discrete profile:
    - that discrete profile is renamed
    - the protection of your backup data set falls to generic profiles that match the backup data set name
      - Which could be no profile, which would expose your RACF backup data set if your have something other than PROTECTALL(FAIL) in effect.
- Running the RACF_SENSITIVE_RESOURCES health check immediately after performing a RENAMEACTIVATE verifies that at least a baseline set of protection exists

Summary

- The path to an encrypted RACF RACF database is a journey

- As stated in the RACF Database Encryption statement of direction, the encryption of the RACF database will be accomplished by leveraging the existing pervasive encryption support for VSAM linear data sets

- Clients can get familiar with a VSAM RACF dataset in V2R5
  - Please be sure to abide by the limitations stated earlier

Appendix: Planned Publication Updates

- Security Server RACF Callable Services
  - No changes

- Security Server RACF Command Language Reference
  - RVARY implications of switching to/from VSAM data set

- Security Server RACF Data Areas
  - Updates for data set-related control blocks (DSDT and friends) as well as the ICB
- Security Server RACOUTE Macros Reference
  - No changes

Appendix: Planned Publication Updates..

- Security Server RACF Security Administrator's Guide
  - Description of how to set up encryption for the RACF data base
  - Specification of REGION=0M on utility examples

- Security Server RACF General User's Guide
  - No changes

- Security Server RACF Messages and Codes
  - Numerous changes for utility, initialization, and manager messages

Appendix: Planned Publication Updates...

- Security Server RACF System Programmer's Guide
  - Description of the overall RACF VSAM support, including what is supported as the support evolves over time
  - Information and considerations on the allocation of the VSAM data
  - Description of the impact of a VSAM data set on the backup and recovery process
  - Description of the updates to IRRUT200, such as RENAMEACTIVATE
  - Discussion of limitations of IRRUT400 with a VSAM data set
  - Description of function and the migration path
  - Specification of REGION=0M on utility examples
  - Changing DISP=OLD to DISP=SHR on several utility examples

Appendix: Planned Publication Updates…

- Security Server RACF Macros and Interfaces
  - No changes
- Security Server RACF Diagnosis Guide
  - Chapter 2 (“Collecting and analyzing problem data”): Collecting the (new) IRR05417I message and any other diagnostic information that might be useful (such as a LISTCAT ENT(racf-ds-name))
  - Chapter 4 (“Troubleshooting your RACF database”): Addition of information that describes the nature of the RACF VSAM data set support and identify any specific VSAM considerations.
  - Chapter 5 (“Diagnosis Reference for RACF”): Addition of specific diagnostic actions that are to be taken
- Security Server RACF Auditor’s Guide
  - Discussion of impact of encryption on RACF database, when that function is available