IBM Education Assistance for z/OS V2R3

Line Item Name: Encrypting Access Methods
Element/Component: RACF

Agenda

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

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- The objective of this session is to describe the changes made to RACF for Encrypting Access Methods. Support is rolled back to V2R1.
  - ICSF segment updates are RACF APAR OA50367 and SAF APAR OA50401
  - DFP segment updates are RACF APAR OA50512
    - template updates are in OA50367 but are not externalized

Overview

- DFSMS currently supports disk data encryption:
  - Software encryption provided with IDCAMS REPRO ENCIPHER/DECIPHER (very limited)
  - For more sophisticated techniques, cryptographic hardware and RACF is required.
- Would like to enhance this capability
  - Application transparency required
    - No application changes or awareness that BSAM/QSAM/VSAM data is encrypted
  - Enhance data security
    - User requires access via the data set profile
    - Discretionary access control by the owner of the data
  - AND for sensitive data -- access to the key that is used by the access method to encrypt and decrypt the data
    - Adds a second access control check
    - Security Administrator must grant access to the key label

Overview

- Can use RACF to protect and control the use of SMS classes, data sets, functions, options, and commands.
- RACF provides the following facilities to support DFP:
  - Supplied general resource classes that you can use to protect SMS classes
    - RACF general resource classes are not the same as SMS classes
  - DFP segment in both user and group profiles in which you can specify default information that DFP uses to determine data management and storage characteristics for data sets
  - DFP segment in data set profiles in which you can specify the owner of SMS-managed data sets protected by the profile
  - Field-level access checking to provide security for fields in the DFP segment of user, group, and data set profiles

Usage & Invocation

- Extends the RACF dataset profile DFP segment
  - Label of an existing key in the ICSF CKDS used for encrypting/decrypting sequential and VSAM data
  - Provides granularity for different key labels to be used based on RACF profiles
  - Key label only used for new data set create
    - ADDSD 'PROJECTA.DATA.*' ... DFP(... DATAKEY(Key-Label))
    - ALTDSD 'PROJECTA.DATA.*' ... DFP(... DATAKEY(Key-Label))
- Extend the CSFKEYS profile ICSF segment
  - Additional field SYMCPACFRET
    - Indicates whether a key label covered by this profile can be returned to the caller in the CPACF-wrapped form (protected key)
    - RDEFINE CSFKEYS AES.APP1.* ICSF(SYMCPACFRET(YES))
    - RALTER CSFKEYS AES.APP1.* ICSF(SYMCPACFRET(YES))

Usage & Invocation

- Add support for conditional access list for CSFKEYS profiles
  - Allows DFSMS to be permitted without granting access to all users of a dataset
    - PERMIT some.label CLASS(CSFKEYS) ID(*) ACCESS(READ) WHEN(CRITERIA(SMS(DSENCRYPTION)))
- R_admin is updated to handle these new fields
- RACROUTE will handle the new criteria

Interactions & Dependencies

- Software Dependencies
  - ICSF (WD#12 [HCR77A0] and up)
  - DFSMS (and subcomponents)
- Hardware Dependencies
  - None
- Exploiters
  - None that aren't already listed in Software Dependencies

Migration & Coexistence Considerations

- These APARs are required for coexistence/toleration:
  - RACF APAR OA50367
  - SAF APAR OA50401
  - RACF APAR OA50512

Installation

- Support is present in the base of z/OS V2R3
- Enablement on older releases will require the same APARs listed before for toleration.
- It is recommended to run:
  - IRRMIN00 PARM=UPDATE
  - IRRMIN00 PARM=ACTIVATE

Session Summary

- Updated ADDSD/ALTDSD (added DATAKEY field to DFP segment in DATASET profiles)
  - This allows a default CKDS key label to be define for newly created datasets
- Updated RDEFINE/RALTER (added SYMCPACFRET field to ICSF segment in CSFKEYS profiles)
  - This allows ICSF to decide whether a protected key may be returned to an “authorized” caller or not
- Updated PERMIT (added SMS(DSENCRYPTION) to WHEN(CRITERIA(...)))
  - This will allow DFSMS to check for access to a label using conditional access list and removing the need to allow users access to the key label
- R_admin support

Appendix

Publication references

- Security Server RACF Callable Services
- Security Server RACF Command Language Reference
- Security Server RACROUTE Macros Reference
- Security Server RACF Security Administrator's Guide
- Security Server RACF System Programmer's Guide
- Security Server RACF Macros and Interfaces
- Security Server RACF Messages and Codes