z/OS 2.5 IBM Education Assistant

Solution Name: Restrict profile management for users with ALTER access

Element(s)/Component(s): RACF

July 2021

Agenda

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

Trademarks

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

Session Objectives

- Understand how ALTER access allows discrete profile management
- Understand how that behavior can now be restricted or outright eliminated

Overview

- Who (Audience)
  - Security administrators, auditors, and application designers
- What (Solution)
  - A security administrator can define a FACILITY profile to prevent users with ALTER access to a discrete profile from managing the profile
  - Exceptions can be made
- Wow (Benefit / Value, Need Addressed)
  - Eliminates one vector for an insider attack
  - Easily provable to auditors
  - Application designers need no longer worry about incorporating ALTER access into their security designs

Usage & Invocation

- These are the ways in which a user might have ALTER access to a discrete profile:
  - A user ID access list entry with ALTER
  - A group access list entry with ALTER
  - An access list for ID(*) with ALTER
  - A universal access of ALTER
  - ALTER access to a matching GLOBAL class member

Usage & Invocation …

- Here’s what ALTER access to a discrete profile allows you to do:

  ---------- list/copy access lists -----------

  - list the access list (RLIST AUTHUSER, LISTDSD AUTHUSER, R_admin profile extract)
  - copy the access list from another profile (RDEFINE FROM, ADDSD FROM, PERMIT FROM) to which you have ALTER access

  ---------- modify/delete profiles ---------

  - modify (RALTER, ALTDSD) the base segment of the profile, excluding the OWNER keyword.
  - modify the access list (PERMIT)
  - delete the profile (RDELETE, DELDSD)

  ---------- Create ‘conflicts’ ---------------

  - define a discrete GLOBAL entry when you have ALTER access to the matching ‘base class’ profile
  - define a matching grouping class member when you have ALTER access to the discrete member class profile
  - define a discrete member class profile when you have ALTER access to a grouping class profile that has a matching member (also requires CLAUTH)
  - define a discrete member class profile, or grouping class member, when you have ALTER access to a generic profile which currently covers the discrete name

Usage & Invocation … Define the control

- The IRR.ALTER.*class-name* resource in the FACILITY class controls ability of ALTER access to confer management rights to the corresponding discrete profile.
- Not defining the profile, or defining it with a universal access of UPDATE access allows continuance of existing behavior.

- To completely eliminate the behavior:

```
RDEFINE FACILITY IRR.ALTER.* UACC(NONE)
```

- To allow the behavior for user ANDREW, but only for the LOGSTRM class:

```
RDEFINE FACILITY IRR.ALTER.LOGSTRM UACC(NONE)
PERMIT IRR.ALTER.LOGSTRM CLASS(FACILITY) ID(ANDREW) ACCESS(UPDATE)
```

Usage & Invocation … Required profile prefix

- The covering profile must start with “IRR.ALTER.”
- This avoids a migration action in the event you have an existing backstop FACILITY profile (e.g. ** or IRR.*) with UACC(NONE), which would otherwise change the default behavior on your system.

Usage & Invocation … Miscellaneous rules

- If you use a discrete profile like IRR.ALTER.APPL, there is no reason to ever assign ALTER access, so don’t!
  - Or they will be able to change the profile and subvert your protection!
- For member/grouping profiles, use the member class name (e.g. TERMINAL). RACF will not generate a check against the grouping class/profile (e.g. GTERMINL) *when authorizing members*.
  - But will if making non-member changes to the grouping profile
- Similar for the GLOBAL class. Checks are made in the ‘base’ class (the class identified by the GLOBAL profile name) when authorizing members.
  - But GLOBAL is checked if making non-member changes to the GLOBAL profile
- Classes sharing the same POSIT number in the Class Descriptor Table need separate exceptions (RACF variables can help)

Usage & Invocation … Logging and detection

- When RACF performs the authorization check to IRR.ALTER.class-name, only successes are logged, and the log string will contain the class and name (in its entirety) of the profile being listed/modified by the command processor (or R_admin)
- Unfortunately, this cannot be used as a completely reliable measure of who is using ALTER access for profile management, as the commands sometimes make the check up front (before checking other authorities), or solely to determine profile ownership (i.e. false positives)
  - WARNING mode is not fully effective for the same reason
- RACF already ships a sample IRRICE query (named “ALDS”) to locate instances of ALTER access in discrete profile access lists. This query could be modified to support general resources.

Interactions & Dependencies

- To exploit this item, all systems in the Sysplex must be at the new z/OS level: No
- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Upgrade & Coexistence Considerations

- None

Installation & Configuration

- N/A

Summary

- ALTER access in discrete profiles can cause separation of duties issues, in that it allows management of the profile itself.
- The entire behavior can be quickly eliminated by defining IRR.ALTER.* with UACC(NONE) in the FACILITY class and RACLIST-refreshing the class.
- If you really do want to maintain the behavior for certain use cases, it can be scoped down to certain classes.

Appendix

- z/OS Security Server RACF Command Language Reference
- z/OS Security Server RACF Security Administrator's Guide