Privileged Users in a RACF-protected z/OS System

KOIRUG and RUGONE - November 2017

Introduction: The Kentucky-Ohio-Indiana RACF Users Group (KOIRUG) and the RACF Users Group of the Northeast (RUGONE) held independent meetings in November of 2017. A roundtable discussion was conducted at each meeting on the topic of which users should be considered "Privileged" in a RACF-protected z/OS environment. Participants at the meetings made suggestions as to what authorities and permissions users might have that would make them "Privileged". This paper presents the combined results of these discussions.

There are four categories of authorities and permissions that could result in a user being considered "Privileged".

- Ability to change security controls
- Access to sensitive data ("sensitive" includes data that is PII, PCI, legally protected, government classified, or company confidential)
- Ability to change the system configuration, especially those related to integrity features
- Ability to circumvent monitoring and detection

The sections that follow provide detailed lists of the specific authorities and permissions related to each of these categories.

Ability to Change Security Controls:

- System-SPECIAL authority
- Group-SPECIAL authority if the scope of groups includes Privileged users and sensitive resources
- System-AUDITOR authority
- System-OPERATIONS authority (can create group dataset profiles)
- Group-OPERATIONS authority if the scope of groups includes sensitive datasets
- UPDATE access to FIELD class resources, especially OMVS UID and GID
- Group connect AUTHORITY other than USE if the group has sensitive datasets or access permissions to sensitive resources
- CLAUTH authority if the class controls access to sensitive resources
- Profile Owner of a Privileged user, a group granting access to sensitive resources, or a privileged or sensitive resource profile
- READ or greater access to FACILITY IRR.PASSWORD.RESET or IRR.PWRESET-prefixed resources profiles encompassing Privileged users
- UPDATE or greater access to FACILITY IRR.DIGTCERT-prefixed profiles
- ALTER access to a discrete profile protecting a privileged or sensitive resource
- Unix Superuser authority
    - UID(0)
    - READ access to FACILITY BPX.SUPERUSER
    - READ access to UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS
    - READ access to UNIXPRIV SUPERUSER.FILESYS.CHOWN
- DB2 SYSADM authority, granted either by the DB2 catalog or READ access to DSNADM db2-subsystem.SYSADM
- Authority to change non-RACF security controls internal to an application processing sensitive data

- Authority to deactivate system software external security options (either by a command or by UPDATE access to configuration datasets)

Access to Sensitive Data:

- READ access to the RACF database and any off-line backups
- System-OPERATIONS authority
- Group-OPERATIONS authority if the scope of groups includes sensitive datasets
- Started Task PRIVILEGED or TRUSTED authority
- System-SPECIAL (access unprotected data)
- Unix Superuser authority
    - UID(0)
    - READ access to FACILITY BPX.SUPERUSER
    - READ access to FACILITY BPX.DAEMON
    - READ or, more importantly, greater access to UNIXPRIV SUPERUSER.FILESYS
    - READ or greater access to UNIXPRIV SUPERUSER.FILESYS.MOUNT
- UPDATE access to Unix ZFS File System datasets
- Access to Storage Administration authorities (can be mitigated by Pervasive Encryption)
    - READ access to FACILITY STGADMIN.ADR.STGADMIN-prefixed resources
    - READ or greater access to DASDVOL resources
    - If either DITTO or File Manager are installed, READ or, more importantly, greater access, especially ALTER, to FACILITY DITTO.DISK.FULLPACK or FILEM.DISK.FULLPACK
- READ or greater access to tape protection bypass authorities
    - Use of Bypass Label Processing (BLP) - FACILITY ICHBLP and Tape Management System specific resources
    - Use of DD EXPDT=98000 - Tape Management System specific resources
- DB2 SYSADM authority, granted either by the DB2 catalog or READ access to DSNADM db2-subsystem.SYSADM
- READ access to z/OS system dump datasets
- Very broad permissions, such as READ access to all JESSPOOL profiles

Ability to change the system configuration:

- UPDATE access to Authorized Program Facility (APF), PARMLIB, LINKLIB, IPL LOAD PARM, and other z/OS system software library datasets
- UPDATE access to FACILITY CSV-prefixed resources
- READ access to FACILITY BPX.FILEATTR-prefixed resources
- UPDATE access to OPERCMDS MVS.SETPROG or MVS.SET.PROG

Ability to circumvent monitoring and detection:

- System-AUDITOR authority
- UPDATE access to SMF datasets, including archives
- UPDATE access to PARMLIB datasets containing the SMF configuration
- UPDATE access to OPERCMDS MVS.SET.SMF or MVS.SETSMF.SMF
- Authority to change data collection options for a SIEM

- Authority to change non-RACF audit files for an application processing sensitive data

All the above:

- READ access to SURROGAT BPX.SRV.*userid* for a Privileged user with Unix Superuser authorities
- READ access to SURROGAT *userid*.SUBMIT for a Privileged user