RSH CONSULTING

Common Holes in RACF Defenses

RUGONE - May 2013

Robert S. Hansel Lead RACF Consultant R.Hansel@rshconsulting.com 617-969-9050

Robert S. Hansel

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., an IT security professional services firm he established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. He has worked with IBM mainframes since 1976 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

Contact and background information:

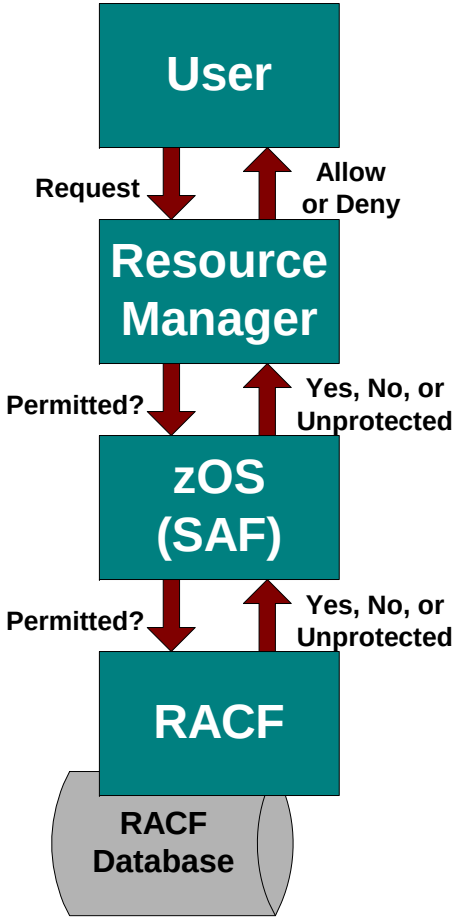
- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- www.rshconsulting.com

Topics

- RACF's Role & Authority
- Logon Control
- Resource Access Control
- Monitoring
- Administration

RACF's Role & Authority

- RACF is called by a system resource manager (e.g. CICS) whenever a user tries to logon or attempts to access a resource
- RACF determines whether an action is authorized and advises the resource manager to allow or disallow the action
- RACF uses the profiles defined in its database to make these determinations
- The resource manager decides what action to take based on what RACF advises
- Common Finding - Resource managers not configured to call RACF
  - Fast Dump Restore (FDR)
  - Connect:Direct
  - CICS



Logon Control

- Inappropriate USERID password options
  - NOINTERVAL No password change required on sensitive IDs
  - PROTECTED Not set for all Started Tasks and Batch IDs
- Weaker passwords RULEs undermining stronger ones
- IBMUSER still has powerful authorities and/or still in use
- JES network and batch logons not properly controlled
  - NODES profiles not restricting inbound NJE from foreign nodes
  - RACFVARS &RACLNDE contains obsolete, inappropriate, or foreign node entries
  - JESINPUT profiles not controlling foreign Ports of Entry (POEs)
  - JESJOBS not enforcing jobname conventions or restricting use of TCP/IP application jobnames (when SERVAUTH PORTACCESS not implemented)
  - RJE signon not using FACILITY RJE.workstation profiles
  - Mandatory batch logon not enforced - JES(BATCHALLRACF) inactive

Logon Control

- SURROGAT profiles inappropriately permit use of privileged IDs
  - Privileged IDs - SPECIAL, OPERATIONS, DB2 SYSADM, Unix uid(0)
  - Unprivileged job submitter acquires authority of surrogate ID
  - CICS SIT parameter XUSER=NO, or improper DFHINSTL and DFHSTART profiles

- PROPCNTL not preventing propagation of IDs onto batch jobs
  - Intended for Job Schedulers, CICS, Automated Operations
  - Submitted jobs acquire ID of submitter instead of Batch IDs
  - Use avoids giving propagated submitter's ID expanded authority to accommodate access needs of all associated batch jobs

Logon Control

- APPL class profiles not guarding or monitoring entry into system applications that should be restricted (e.g., CICS test, Tivoli Workload Scheduler (TWS), Netview)
- Process IDs used from multiple purposes (e.g. Batch, FTP, and Started Task)
- Started Tasks not uniquely identified for individual control
  - Problematic if IDs are shared by multiple unrelated Started Tasks
  - Shared IDs must be given expanded authority to accommodate access needs of all associated Started Tasks
- Failure to implement SSL/TLS to avoid transmission of passwords in clear text

Resource Access Control

- Resource classes inactive or not fully implemented
  - TEMPDSN
  - MQ-related classes
  - SDSF and related classes (using ISFPARMs instead of RACF)
  - WRITER (not restricting outbound NJE transmissions)
  - LOGSTRM
  - SERVAUTH
  - DB2-related classes (using DB2 catalogs instead of RACF)
  - FACILITY (see RSH "FACILITY Class" presentation)
  - RACLIST-required classes active but not RACLISTed (e.g., SERVAUTH, UNIXPRIV)

- PROGRAM class
  - ** profile with UACC(READ), needed for z/OS Unix, also grants access to ICHDSM00, IRRDPI00, and IEHINITT
  - Libraries listed in profiles are obsolete, unneeded, or incomplete
  - ENHANCED protection mode not implemented

Resource Access Control

- UACC or ID(*) allow inappropriate access
  - READ/UPDATE or above for datasets
  - READ or above for general resources

- Global Access Table entries allow access prohibited by the resource profile

GAT Entry	SYS1.**	READ
Profile	SYS1.RACF.**	NONE

- WARNING
  - Left on for excessive length of time (and not monitored)
  - Applied to inappropriate resources

- RESTRICTED attribute not set on external and default IDs

- Dataset Erase-on-Scratch (ERASE) not implemented

Resource Access Control

- Unnecessary or inappropriate access permissions to system datasets
  - PARMLIBs - Deactivate tape security; add APF authorized libraries
  - APF libraries - Programs can circumvent controls
  - Linklist libraries - May be Authorized; Trojan horse attack risk
  - PROCLIBs - Started Task PROCs open to manipulation or subversion
  - RACF datasets - Backups often unprotected
  - Catalogs - Excessive ALTER access
  - SMF datasets - Integrity of archives not protected

Resource Access Control

- Storage administration authorities not set up properly
  - OPERATIONS attribute assigned extensively and used excessively
  - No OPERATIONS authority access blocking group created or properly used
  - DASDVOL profiles either not used or grant excessive authority
  - FACILITY STGADMIN profiles either not used, not fully defined, or grant excessive authority (especially those protecting STGADMIN.ADR.STGADMIN resources)
  - FACILITY DITTO.DISK.FULLPACK grants excessive authority
  - Tape BLP and EXPDT=98000 security bypass not properly controlled

- Installation-defined entries in the Program Property Table (PPT) inappropriately assign NOPASS attribute, especially to DFHSIP

Resource Access Control

- Installation-defined classes honor OPERATIONS authority

- Inappropriate access granted to system administration resources
  - System control and configuration commands and functions
    - OPERCMDS
    - FACILITY CSV-prefixed, MVSADMIN, ...
    - TSO authorities - TSOAUTH OPER, ACCT, PARMLIB, CONSOLE, and TESTAUTH
  - CICS commands
    - Class 1 and 2 transactions (e.g., TCICSTRN CEMT, CEDF, CEDA, etc.)
    - CCICSCMD / VCICSCMD resources - SIT parameter XCMD=NO
    - DFLTUSER permissions

Resource Access Control

- z/OS Unix identities, authorities, and permissions not properly controlled
  - Unix service routines (daemons) unnecessarily permitted access to FACILITY BPX.DAEMON
  - Unnecessary assignment of uid(0) to both daemons and Tech Support staff
  - Under utilization of UNIXPRIV authorities as replacement for uid(0)
  - Inappropriate access granted to …
    - FACILITY BPX.SUPERUSER
    - FACILITY BPX.FILEATTR.APF
    - UNIXPRIV SUPERUSER.FILESYS
  - OMVS uids and gids shared
  - UNIXPRIV SHARED.IDS not defined to prevent duplicate uid and gid assignments
  - Continue reliance on BPX.DEFAULT.USER
  - BPX.DEFAULT.USER Unix Default User is set as OWNER of files and directories
  - OTHER granted excessive permissions, especially Write (w) to directories
  - UNIXPRIV RESTRICTED.FILESYS.ACCESS not defined to block RESTRICTED user access to OTHER permissions
  - Extended Access Control Lists (ACLs) not used effectively

Resource Access Control

- Started Tasks unnecessarily given PRIVILEGED or TRUSTED
  - Grants unrestricted access to nearly all resources
    - Access any dataset or DASD volume
    - Use any command, function, or resource
    - Submit jobs with any other ID as surrogate
    - Gain Unix Superuser uid(0) authority
  - Limited monitoring - TRUSTED alone can be logged, but only with LOGOPTIONS(ALWAYS) or UAUDIT

  - IBM recommended TRUSTED Started Tasks

(1) Optional

APSWPROx(1)	CATALOG	CEA	DFHSM(1)	DFS(1)
DUMPSRV	GPMSERVE(1)	HIS	IEEVMPCR	IOSAS
IXGLOGR	JESn	JESXCF	LLA	OMVS(1)
NFS	RACF	RMF	RMFGAT	SMF
SMS	SMSVSAM(1)	TCPIP	VLF	VTAM
XCFAS				

Monitoring

- SETROPTS monitoring options are not active
  - OPERAUDIT not active
  - AUDIT(class) not set for all classes
  - LOGOPTIONS(FAILURES(class)) not set for all classes, especially z/OS Unix related classes PROCESS, PROCACT, IPCOBJ
  - LOGOPTIONS(ALWAYS(FSSEC)) not set

- Profile AUDIT options are not set to capture important events
  - Resource profiles lack AUDIT(FAILURES(READ)) to record violations
  - Critical resource profiles do not have AUDIT(SUCCESS(*level*)) to monitor sensitive access
    - System dataset UPDATE
    - Use of SURROGAT authority for privileged IDs
  - Sensitive or semi-trusted IDs do not have UAUDIT attribute
    - Privileged or non-employee IDs (e.g. contractors)

Monitoring

- Reporting tools not used effectively
  - Incomplete SMF input data selected
    - All pertinent record types not processed
    - Data from all system images not included
  - Record selection criteria is not comprehensive
    - Only certain Violation events requested
    - Warning and Successes not selected
  - Reports on important types of activities not generated
    - Access to sensitive and critical resources
    - Warnings
    - Activities of UAUDIT users
    - Logons by undefined users
    - OPERATIONS and Storage Admin authority use
    - Security administration actions
  - Reports not organized for efficient review
  - Reports not disseminated to user and resource owners
- SMF data retention too short for research and analysis of past events

Administration

- Inappropriate assignment of User and Group authorities
  - User and Connect GRPACC and ADSP attributes
  - Group CREATE, CONNECT, and JOIN authorities
  - Class authorization (CLAUTH) assigned but not used
  - AUDITOR authority given to staff other than Audit or Security
  - SPECIAL authority assigned to batch and Started Task IDs
  - Profile ownership not properly assigned
- ALTER access granted to Discrete profiles when not required
- Access lists contain obsolete entries - IRRRID00 and IRRHFSU not run regularly
- Entry of RACF commands via the console not tested regularly
- RACF Database not backed up using IRRUT200
- Underutilization of performance enhancement features

Administration

- No coordination of RACF ID management with other systems
  - HR interface to manage user transfers and terminations
  - z/OS Unix File System OWNER, GROUP, and ACLs
  - DB2 Catalog grants
  - ViewDirect Recipient IDs
  - NetView Access Services IDs
  - Application internal tables
- Resource owners not assigned or involved in granting access
- Group architecture, naming standards, and role-based access are not clearly defined or adhered to
- No formal Mainframe/RACF security policy or standards
- RACF administration function understaffed and undertrained

Conclusion

All Installations Have Issues!

You are not alone