RSH

CONSULTING

Common Holes in RACF Defenses

IBM Systems TechU - October 2018

RSH CONSULTING, INC. • RACF SPECIALISTS • 617-969-9050 • WWW.RSHCONSULTING.COM

RSH Consulting - Robert S. Hansel

RSH Consulting, Inc. is an IT security professional services firm 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. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

z/OS Security

- How important is the z/OS mainframe's data and services to your organization

- How would your organization be affected if data on the mainframe was ...
  - Stolen or publicly disclosed
  - Inappropriately modified
  - Deleted
  - Rendered unavailable because the operation of the system was disrupted

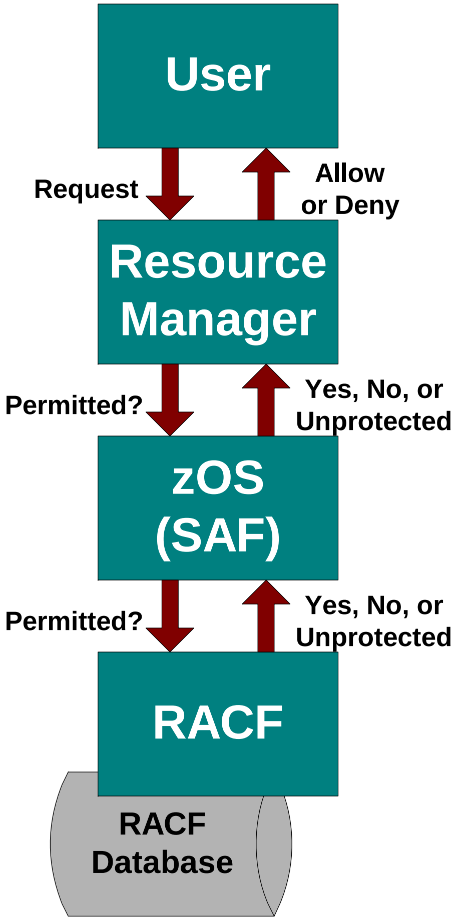
- Working in conjunction with z/OS and installed system software products (e.g., CICS), RACF can help guard against bad outcomes by preventing users from accessing data and software functions they are not supposed to use *if it is fully and properly implemented*

Topics

- RACF’s Role and Authority
- Logon Control
- Resource Access Control
- Monitoring
- Administration

RACF’s Role and 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



Logon Control

- Stronger password protection not used to thwart brute-force password guessing attacks
  - KDFAES encryption algorithm
  - Mixed-case passwords
  - Password phrases
  - Multi-Factor Authentication (MFA)
- Password MINCHANGE not used to prevent password recycling
- PROTECTED attribute not assigned to Batch and Started Task IDs
  - No password to disclose or misuse
  - Prevents ID from becoming REVOKED
- PROPCNTL not used to prevent Started Task ID propagation to batch jobs, especially the job scheduler

Logon Control

- SURROGAT profiles permit inappropriate use of IDs
  - Batch
    - SURROGAT *userid*.SUBMIT profiles allow a user to submit jobs with another user's ID and indirectly acquire the authority of the other ID
    - Often allow questionable use of privileged IDs - SPECIAL, OPERATIONS, DB2 SYSADM, Unix uid(0)
  - CICS
    - SIT parameter XUSER set to NO - no restriction on IDs assigned for default, terminal, etc.
    - When XUSER=YES, *userid.*DFHINSTL and *userid.*DFHSTART profiles are not strict

- JES NJE connections and inbound work are not properly controlled
  - NODES profiles either not restricting inbound NJE transmissions from foreign nodes or inappropriate 'trusting' foreign nodes
  - RACFVARS &RACLNDE profile - defines 'trusted' nodes and supersedes NODES restrictions - contains obsolete or inappropriate entries
  - JESINPUT profiles not controlling which IDs can be used on batch jobs from foreign Ports of Entry (POEs)

Resource Access Control

- Resource classes inactive or not fully implemented
  - TEMPDSN - not active; therefore, access to residual temporary datasets is allowed
  - WRITER - not restricting outbound NJE transmissions
  - VTAMAPPL - not active or no profiles restricting the opening of VTAM ACBs
  - SERVAUTH - not protecting TCP/IP network resources
  - FACILITY - not guarding all resources (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, grants access to ICHDSM00, IRRDPI00, and IEHINITT
  - Libraries listed in profiles are obsolete, unneeded, or incomplete
  - ENHANCED protection mode not implemented

- Dataset Erase-on-Scratch (ERASE) not implemented
  - Pervasive Encryption a viable alternative

Resource Access Control

- UACC or ID(*) allow inappropriate access
  - READ/UPDATE or above for datasets - especially for sensitive data
  - 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

- For SDSF, users not restricted to using operator commands (OPERCMDS) only from within SDSF - PERMIT WHEN(CONSOLE(SDSF))

Resource Access Control

- Unnecessary or inappropriate access permissions to system datasets

• APF libraries	- Programs can be inserted that can circumvent controls
• PROCLIBs	- Started Task PROCs open to manipulation or subversion
• RACF datasets	- Backups often unprotected
• Catalogs	- Excessive ALTER access
• SMF Data	- Alter audit trails; disclose passwords mistakenly entered as ID
• Unix File Systems	- Alter security bits

- Storage administration authorities not set up properly
  - OPERATIONS attribute assigned extensively and used excessively
    - No use of restrictive permissions to curb OPERATIONS authority (e.g., Catalogs)
    - Installation-defined classes honor OPERATIONS authority
  - FACILITY STGADMIN profiles either not used, not fully defined, or grant excessive authority (especially those protecting STGADMIN.ADR.STGADMIN resources)
  - DASDVOL profiles not defined when FDR is installed
  - Tape BLP and EXPDT=98000 security bypass not properly controlled

Resource Access Control

- No 'catch-all' ** profile defined for General Resource classes potentially leaving some resources unprotected (excluding FACILITY, UNIXPRIV)

- Inconsistencies in access controls for data on DASD shared by systems with different RACF databases

- Inappropriate access to SET and HALT type operator commands (OPERCMDS)

- Inappropriate access granted to CICS commands
  - New Class 1 and 2 transactions in latest release not properly protected
  - SIT parameter XCMD= set to NO - no use of CCICSCMD / VCICSCMD resources controls

Resource Access Control

- z/OS Unix identities, authorities, and permissions not properly controlled
  - Unix service routines (daemons) and technical support users unnecessarily permitted access to FACILITY BPX.DAEMON
  - Unnecessary assignment of uid(0) to both daemons and Tech Support staff
  - Under utilization of FACILITY BPX.SUPERUSER and UNIXPRIV authorities as replacement for uid(0)
  - Inappropriate access granted to …
    - FACILITY BPX.SUPERUSER
    - FACILITY BPX.FILEATTR.APF
    - UNIXPRIV SUPERUSER.FILESYS
  - OTHER granted excessive permissions, especially Write (w) to directories
  - UNIXPRIV RESTRICTED.FILESYS.ACCESS not defined to block RESTRICTED user access to OTHER permissions
  - SETUID enabled for mounts of Unix File System datasets under user control
  - Access to Unix and TCP/IP applications open to all users (e.g., FTP)

Resource Access Control

- Started Tasks unnecessarily given PRIVILEGED or TRUSTED
  - TRUSTED should only be assigned to the following tasks as recommended by IBM

APSWPROx[1]	CATALOG	CEA[2]	DFHSM[1]	DFS[1]
DUMPSRV	GPMSERVE[1]	HIS	IEEVMPCR	IOSAS
IXGLOGR	JESn	JESXCF	JES3AUX	LLA
NFS	OMVS[1]	RACF	RMF	RMFGAT
SMF	SMS	SMSPDSE1	SMSVSAM[1]	TCPIP
VLF	VTAM	WLM	XCFAS	ZFS[1]

(1) Optional (2) If using z/OSMF ISPF

Monitoring

- SETROPTS monitoring options are 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 and warnings
  - 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 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 authorities
  - Group CREATE, CONNECT, and JOIN authorities
  - AUDITOR authority given to staff other than Audit or Security (new - ROAUDIT)
  - 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

Administration

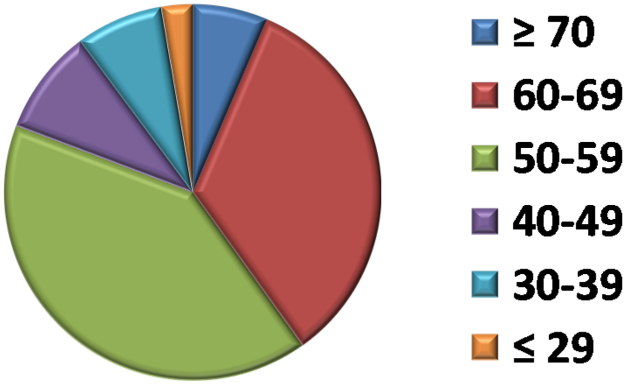
- No coordination of RACF ID management with other systems
  - HR interface to manage user transfers and terminations
  - z/OS Unix File System OWNER, GROUP, and ACLs
  - DB2 Catalog grants
  - ViewDirect Recipient IDs
  - NetView Access Services IDs
  - Application internal tables
- Resource owners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

Administration

Survey of RACF-L Participants - November 2017

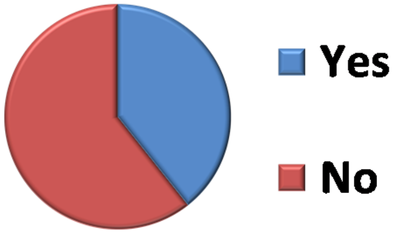
What is your age group?

Responses	Count	Percent %
70 and above	12	6.4%
60-69	63	33.7%
50-59	76	40.6%
40-49	17	9.1%
30-39	14	7.5%
29 and below	5	2.7%
Total	187	100%



Are you planning to retire in the next 5 years?

Responses	Count	Percent %
Yes	72	39.3%
No	111	60.7%
Total	183	100%



Conclusion

All Installations Have Issues!

You are not alone