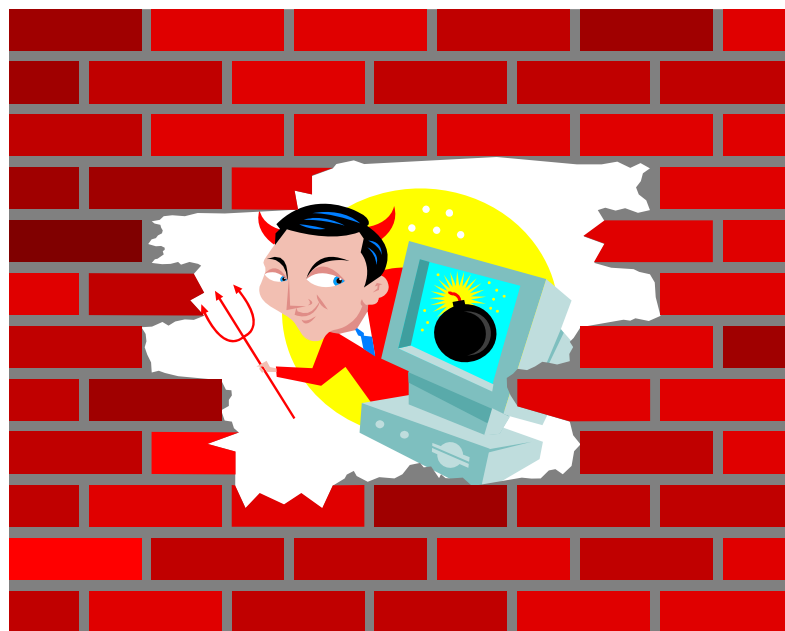


# ***COMMON HOLES IN RACF DEFENSES***

**Vanguard Security & Compliance 2011 - CAR10 - June 2011**



**Robert S. Hansel**

**Lead RACF Specialist - RSH Consulting, Inc.**

**R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com**

# RSH PRESENTER



**Robert S. Hansel** is Lead RACF Specialist and founder of RSH Consulting, Inc., a 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 1977 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](mailto:R.Hansel@rshconsulting.com)
- [www.linkedin.com/in/roberthansel](http://www.linkedin.com/in/roberthansel)

# *TOPICS*

**RACF's Role & Authority**

**Logon Control**

**Resource Access Control**

**Monitoring**

**Administration**

RACF and z/OS are Trademarks of the International Business Machines Corporation

# 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

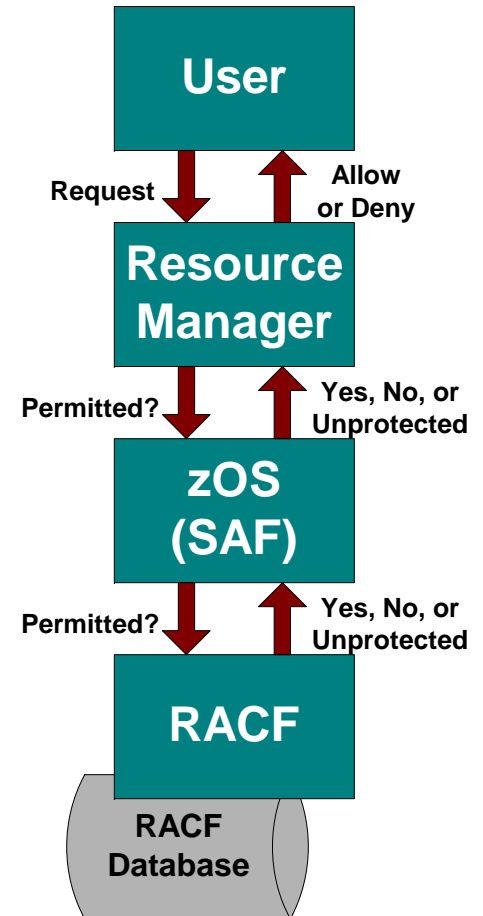
RACF determines whether an action is authorized and *advises* the resource manager to allow or disallow the action

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

## **JES resources and batch logons not properly controlled**

- **NODES** profiles not restricting inbound NJE from foreign nodes
- **RACFVARS &RACLNDE** contains obsolete or foreign node entries
- **JESINPUT** profiles not controlling foreign Ports of Entry (POEs)
- **WRITER** profiles not restricting outbound NJE to foreign nodes
- **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 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, including TCP/IP applications and Tivoli Workload Scheduler (TWS)**

**Process IDs used from multiple purposes (e.g. Batch, FTP, 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 and not fully implemented**

- **VTAMAPPL**
- **LOGSTRM**
- **SERVAUTH**
- **TEMPDSN**
- **MQ-related classes**
- **SDSF & JES-related classes (using ISFPARMs)**
- **DB2-related classes (using DB2 catalogs)**
- **FACILITY (see RSH "FACILITY Class" presentation)**

## **PROGRAM class**

- **Not active**
- **\*\* 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**

# 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**

<b>GAT Entry</b>	<b>SYS1.**</b>	<b>READ</b>
<b>Profile</b>	<b>SYS1.RACF.**</b>	<b>NONE</b>

## **WARNING**

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

**RESTRICTED attribute not set on external & default IDs**

# **RESOURCE ACCESS CONTROL**

## **Unnecessary or inappropriate permits to system datasets**

- **PARMLIBs** - Deactivate tape security; authorize libraries
- **APF libraries** - Programs can circumvent controls
- **Linklist libraries** - May be Authorized; Trojan horse attack risk
- **RACF datasets** - Backups often unprotected
- **Catalogs** - Excessive ALTER access
- **PROCLIBs** - Stated Task PROCs open to subversion
- **SMF datasets** - Integrity of archives not protected

# **RESOURCE ACCESS CONTROL**

## **Storage administration authorities not set up properly**

- **OPERATIONS** attribute assigned extensively and used excessively
- **DASDVOL** profiles either not used or grant excessive authority
- **FACILITY STGADMIN** profiles either not used, not fully defined, or grant excessive authority
- **FACILITY DITTO.DISK.FULLPACK** grants excessive authority
- **Tape BLP** and **EXPDT=98000** security bypass not properly controlled
- **ISMF** programs are not protected

**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**

- **Operator commands**
  - **OPERCMDS**
  - **FACILITY CSV-prefixed, MVSADMIN, ...**
  - **SDSF**
- **CICS commands**
  - **TCICSTRN CEMT, CEDF, CEDA, etc.**
  - **CCICSCMD / VCICSCMD resources**
  - **CICS DFLTUSER permissions**
- **TSO authorities - TSOAUTH OPER, ACCT, PARMLIB, & CONSOLE**

# **RESOURCE ACCESS CONTROL**

## **z/OS Unix identities and authorities not properly controlled**

- **Unix service routines unnecessarily permitted access to FACILITY BPX.DAEMON**
- **OMVS uids and gids assignments not unique**
- **Unnecessary assignment of uid(0)**
- **Inappropriate access granted to FACILITY BPX.SUPERUSER**
- **Under utilization of UNIXPRIV authorities**
- **Extended 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
  - Limit monitoring - TRUSTED alone can be logged, but only with LOGOPTIONS(ALWAYS) or UAUDIT

- IBM recommended TRUSTED Started Tasks

(1) Optional

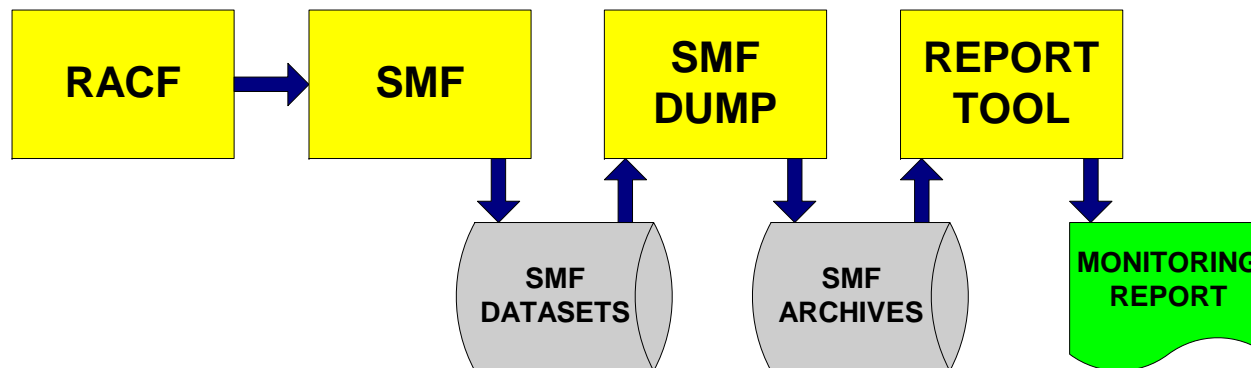
APSWPROx <sup>(1)</sup>	CATALOG	DFHSM <sup>(1)</sup>	DFS <sup>(1)</sup>
DUMPSRV	GPMSEVE <sup>(1)</sup>	IEEVMPER	IOSAS
IXGLOGR	JESn	JESXCF	LLA
OMVS <sup>(1)</sup>	NFS	RACF	RMF
RMFGAT	SMF	SMS	SMSVSAM <sup>(1)</sup>
TCPIP	VLF	VTAM	XCFAS

# MONITORING

Reporting tools require comprehensive SMF data collection and retention to be effective

## Log collection & reporting process

- Resource Manager calls RACF for authorization check
- RACF Caller requires or does not suppress logging
- RACF Options Generate SMF Log Record
- SMF Collects and Saves Log Record
- SMF Record is Dumped for Report Processing
- RACF Tools Generate Reports from SMF Record



# MONITORING

## 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)

## 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

# **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**

# **ADMINISTRATION**

## **Inappropriate assignment of User and Group authorities**

- **User and Connect GRPACC and ADSP attributes**
- **Group CREATE, CONNECT, and JOIN authorities**
- **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 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 & terminations**
- **z/OS Unix HFS**
- **DB2 Catalog grants**
- **ViewDirect Recipient IDs**
- **NetView Access Services IDs**
- **Application internal tables**

**Group architecture, naming standards, and role-based access are not clearly defined or adhered to**

**Resource owners not assigned or involved in granting access**

**No formal Mainframe/RACF security policy or standards**

**RACF admin function understaffed and undertrained**

***ALL INSTALLATIONS HAVE ISSUES***

***You are not alone!***