Solving IMS Security Problems

C13 and A16

Maida Snapper
March 18, 2015

IMS Technical Symposium 2015

Disclaimer

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- Exits
- Dependent region security (RAS)
- References

Areas We Will Explore

- **Security Activation**
- RACF resource class and profile
- User ID
- Exits
- Dependent region security (RAS)
- References

The APPL Gate

Security Activation Concepts (cont)

How is the message trying to get in?

There’s a lock for that.

The “windows”	The keys	Where to find the keys
3270 terminal	RCF	DFSPB
TCO script	RCF and TCORACF	DFSPB
OTMA	OTMASE	DFSPB
ODBA	ODBASE or ISIS	DFSPB
APPC / LU 6.2	APPCSE	DFSPB
MSC	MSCSEC	DFSDC
Operations Manager (OM)	CMDSEC	CSLOI DFSCG or DFSDF
MCS or E-MCS	CMDMCS	DFSPB
DBRC	CMDAUTH	RECON
AOI type 1	AOI1	DFSPB
AOI type 2	AOIS	DFSPB
Dependent region	ISIS	DFSPB

Security Activation Concepts (cont)

CMDSEC in CSLOIxxx for Operations Manager

- Tells OM what security to perform for **all** commands (type 1 and type 2)
- OM only uses the OPERCMDS class
  - Define type 1 commands using OPERCMDS profile format
    - Example to protect /DIS DB command RDEF OPERCMDS IMS.*plxname*.DIS.DB UACC(NONE)
  - OM does not use CIMS class

CMDSEC in DFSCGxxx or DFSDFxxx for IMS

- Tells IMS what security to perform for type 1 commands passed to IMS from OM
  - IMS does not perform security for type 2 commands
- IMS only uses the CIMS class
  - Define type 1 commands using CIMS profile format
    - Example to protect /DIS command RDEF CIMS DIS UACC(NONE)
  - IMS does not use OPERCMDS class

Solving Security Activation Problems

Now let’s solve some problems

Solving Security Activation Problems (cont)

I set RCF=Y but I’m not getting RACF security for everything

- Because RCF=Y only locks the ETO terminal “window”

OK, I changed RCF from Y to A but that didn’t make any difference.

- Because you have to cold start for RCF changes to take effect

Solving Security Activation Problems (cont)

I turned off all security in my test system but I'm still getting security violations when I do some IMS commands.

DFS3662W 17:20:17 COMMAND REJECTED BY DEFAULT COMMAND SECURITY

- Because turning off all security gives you default security which protects some type 1 commands.

Solving Security Activation Problems (cont)

I gave DIS a UACC(READ) so everyone would be authorized but some people can't do /DIS

DFS3662W 17:20:17 COMMAND REJECTED BY DEFAULT COMMAND SECURITY

- Because if you didn't lock one of the windows, commands entered through that window get default security.
- Default security for that window might not allow /DIS

Solving Security Activation Problems (cont)

I turned off AOI security but programs are still getting CD status codes.

- Because even if you aren't using AOI security, you still need to code a value for AOI on the TRANSACT macro in order to allow the transaction to issue DLI CMD calls.

Solving Security Activation Problems (cont)

I set RACF=Y in IMS Connect but unauthorized users are able to do transactions.

- Because IMS Connect can verify a user ID but does not do transaction authorization.

- IMS OTMA does transaction authorization
  - You need to set OTMASE to get transaction authorization for transactions from IMS Connect

Solving Security Activation Problems (cont)

Why isn't Operations Manager calling RACF for type 1 commands?

- OM ***is*** calling RACF for type 1 commands. You did not define type 1 commands in the OPERCMDS class. RACF did not find profiles and gave OM return code 04 ("unprotected"). OM passed the commands to IMS.

- When IMS got the commands from OM, IMS did not call RACF because CMDSEC was not specified in DFSCGxxx or DFSDFxxx.

Solving IMS Security Problems (cont)

Remember:

- Each “window” is locked independently of the rest
- If a “window” is not locked
  - Default security is in effect for type 1 commands entered through that “window”
  - The commands allowed by default are different depending on the “window”
  - If the Command Authorization Exit (DFSCCMD0) is in RESLIB, default security is deactivated
- Locks can be changed with a warm start
  - Exception: RCF requires a cold start to change

Areas We Will Explore

- Security Activation
- **RACF resource class and profile**
- User ID
- Exits
- Dependent region security (RAS)
- References

Class and Profile Concepts (cont)

If you ask for RACF security, then at IMS initialization

IMS calls RACF to load resource profiles into RACF dataspace

RACROUTE REQUEST=LIST,GLOBAL=YES

If this fails: U0166

Class and Profile Concepts (cont)

Some of the default resource classes that come with RACF:

T*IMS*

C*IMS*

I*IMS*

L*IMS*

Class and Profile Concepts (cont)

Default IMS resource classes

- These resource classes may be required for IMS to come up
  - Depends on your security parameters

CIMS | DIMS	Commands (first 3 characters of command)
TIMS | GIMS	Transactions (trancode)
IIMS | JIMS	Program Specification Blocks (PSBs)
LIMS | MIMS	Logical terminals (LTERM)
AIMS	APSB (Allocate PSB) for CPIC-PSB and ODBA

Class and Profile Concepts (cont)

Default IMS resource classes

- These resource classes are not required for IMS to come up
  - Certain function will not be available

RIMS	Asynchronoushold queues for RESUME TPIPE call
FIMS | HIMS	Database fields (for AUTH calls)
SIMS | UIMS	Database segments (for AUTH calls)
OIMS | WIMS	Other (information in RACF for AUTH calls)
PIMS | QIMS	Databases (for AUTH call)

Class and Profile Concepts(cont)

IMS also shares some resource classes with other products

TERMINAL | GTERMINL

APPL

VTAMAPPL

APPCPORT

APPCLU

APPCTP

DATASET

FACILITY

OPERCMDS

STARTED

Class and Profile Concepts (cont)

In a single, shared RACF database you can have different security rules for the same resource

- RACF resource is defined by Class + Name
  - Example: TIMS + ADDINV
- You can define a new class
  - Example: TIMSTEST + ADDINV
- You can point IMS to its own set of RACF rules using RCLASS
  - Example: RCLASS=IMSTEST

IMS General Resource Profiles

IMS resource	Resource class singular/grouping	Resource name
Transaction	T*IMS* / G*IMS*	transaction code
Command (type 1)	C*IMS* / D*IMS*	first 3 characters of command
DBRC command	FACILITY	*safhlq*.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.*plxname*.command_verb.command_keyword
Program (PSB)	I*IMS* / J*IMS*	program name
Logical terminal	L*IMS* / M*IMS*	logical terminal name (lterm)
CF structure	FACILITY	CQSSTR.*structure_name* or IXLSTR.*structure_name*
IMS Control Region	APPL	*Imsid and sapplid*
IMSPlex (CSL)	FACILITY	CSL.*imsplexname*
XCF group (Client bid)	FACILITY	IMSXCF.groupname.*membername*
Dataset	DATASET	*dataset name*

Class and Profile Concepts (cont)

Example of some installation-defined resource classes when RCLASS=IMSTEST

T*IMSTEST*

C*IMSTEST*

I*IMSTEST*

L*IMSTEST*

Sample IMS Resource Class Description for Transactions

TIMS

POSIT=4
OTHER=ALPHANUM
MAXLNTH=8
DFTRETC=4
DFTUACC=NONE
GROUP=GIMS
OPER=NO
ID=9
FIRST=ALPHANUM

GIMS

POSIT=4
OTHER=ALPHANUM
MAXLNTH=8
DFTRETC=4
DFTUACC=NONE
MEMBER=TIMS
OPER=NO
ID=10
FIRST=ALPHA

Class and Profile Concepts (cont)

To have different security rules for different IMS systems you can define your own classes

- Class name 1-8 alphanumerics
  - First character must match corresponding default class
    - C, D, T, G, I, J, L, M, A, R, etc
  - Model new classes on the corresponding default class
    - Length must be the same as default class (8)
    - Optionally change the POSIT value
  - Activate the new classes
    - SETR CLASSACT(*classname)*
  - Point IMS to the new classes
    - Specify RCLASS in DFSPBxxx (default is IMS)
    - RCLASS= position 2-8 of class name

Class and Profile Concepts (cont)

- POSIT value
  - an arbitrary number that ties classes together for operations like activate/deactivate/refresh
  - You can specify POSIT values 19–56 and 128–527.
    - POSIT 0–18, 57–127, and 528–1023 are reserved for IBM

Solving Class and Profile Problems

Now let’s solve some problems

Solving Class and Profile Problems (cont)

Why did IMS abend U0166 at initialization?

- A **required** resource class not active
  - Default classes also need to be activated
  - Deactivated by mistake
- A **required** resource class not defined
  - Maybe RACF ignored it if >1024 classes defined
- Wrong class specified
  - IMS 13: Maybe RCLASS was not specified in PROCLIB
- SAF product not available
  - Maybe not updated to support a new IMS release

Solving Class and Profile Problems (cont)

Why did I start getting this message?

DFS3187W RACF NOT ACTIVE FOR RESUME TPIPE CLASS=RIMS

- Because RACF could not load profiles for RIMS class
  - RIMS secures retrieval of OTMA asynchronous output messages
- IMS functions normally but without security for RESUME TPIPE

Solving Class and Profile Problems (cont)

Should I worry about this?

DFS2466I AUTHORIZATION RACLIST FAILED, RACROUTE= 04, 04, 04, 04 RACLIST= 08, 08, 08, 08
REASON= 00, 00, 00, 00 . IMSA

- RACF could not load profiles for the following classes:
  - FIMS,HIMS,SIMS,UIMS,OIMS,WIMS,PIMS,QIMS
- IMS functions normally but application AUTH calls get A4 status code

Solving Class and Profile Problems (cont)

Why didn’t my RACF changes take effect when I recycled IMS?

- Because recycling IMS has no effect on the RACF dataspace
  - Exception: if you activate a new IMS class, recycle IMS to load it into the RACF dataspace
- Updating a RACF resource profile updates the RACF ***database***.
- You must REFRESH the online RACF ***dataspace***
- Issue REFRESH on all systems sharing the RACF database
  - unless RACF is enabled for sysplex communication
- All classes with the same POSIT value will be refreshed

Solving Class and Profile Problems (cont)

HELP! My RECONs are being discarded!

- Because a user was not authorized to all 3 RECON datasets, VSAM got a RACF violation and told IMS the RECON could not be opened. IMS thought it was an I/O error and discarded it.
- Make sure authorized users are in the access list with an appropriate level of access for all 3 RECON datasets.

Solving Class and Profile Problems (cont)

Remember:

- Bigger is not better
  - Define new classes the same MAXLNTH as the IMS default classes
  - Changing MAXLNTH gives unpredictable results including 0C4
  - MAXLNTH for IMS default classes is 8

- Be careful if sharing POSIT value

- RACF allows conflicting profiles and will use these rules
  - the most *specific* (best match)
  - the most *restrictive* UACC
  - the most *permissive* ACCESS

Solving Profile Problems (cont)

- Undefined = Unprotected
  - RACF return code is 04 for a resource with no profile
  - IMS allows access

- Beware of using Discrete profiles for datasets
  - Discrete profiles are deleted when the dataset is deleted
  - Avoid this problem by using Fully Qualified Generic profiles

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- **User ID**
- Exits
- Dependent region security (RAS)
- References

User ID Concepts

An IMS user ID is not always a person sitting at a terminal…....

An IMS user ID can be for:

- Job, Started Task (BMP, utility, etc.)
- Transaction
- Command
- Logical terminal (LTERM)
- Program (PSB)
- TCO (Time Controlled Operations) script
- IMS Master terminal or system console WTOR

User ID Concepts (cont)

- All IMS regions should have a user ID.
  - Can use RACF STARTED class to assign user ID
  - RACF builds ACEE when region starts
    - This is the “security environment” for that region

- If possible, require all users to sign on.
  - ETO users are required to sign on
  - Static terminal users can be forced to sign on
    - SIGNON=ALL
    - AUTOSIGN
    - WTORUSID
    - MTOUSID

United Kingdom of Great Britain and Northern Ireland

Passport Passeport

Type/Type
P

Code of issuing State/Code de l'Etat émetteur
GBR

Passport No/Passeport No
023477812

Surname/Nom
BEAN

Given name/Prenom
MR

Nationality/Nationalité
BRITISH CITIZEN

Date of birth/Date de naissance
6 JAN/JAN 55

Children/Enfants
0

Sex/Sexe
M

Place of birth/lieu de naissance
ENFIELD

Date of issue/Date de delivrance
20 SEP/SEP 96

Authority/Autorité
UNITED KINGDOM PASSPORT AGENCY

Date of expiry/Date d'expiration
20 SEP/SEP 06

Observations/page/Observation-page

P<GB<MR<BEAN<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<

023477812GBR8111063M0004422<<<<<<<<<<<<<<<<<<<<<<06

User ID Concepts (cont)

- IMS calls RACF for user ID verification and ACEE creation

RACROUTE REQUEST=VERIFY

ENVIRON=CREATE

USERID=*userid*

GROUP=*group*

PASSCHK=YES/NO

PASSWRD=*password*

APPL=*imsid or sapplid*

TERMID=*physical terminal*

STAT=YES/NO/ASIS

ACEE=*addr*

User ID Concepts (cont)

When the user signs off

- IMS calls RACF to delete the user's ACEE
  RACROUTE REQUEST=VERIFY,ENVIR=DELETE,ACEE=addr…

- IMS logs x'16'

User ID Concepts (cont)

Messages from SNA terminal

- ETO user must /SIGN ON

- If static terminal sign on is not required
  - User can /SIGN ON
  - IMS can specify AUTOSIGN
  - If user does not sign on
    - No VERIFY call to RACF, no ACEE is built
    - RACF uses “security environment” (ACEE) of caller (IMS CTL)
    - IMS puts the LTERM in the user ID field of the message

User ID Concepts (cont)

MSC

- Messages from many different IMS users flow across the physical link
- It is a 'pooled connection‘
- IMS includes original user ID from the original msg (from SNA terminal, APPC or OTMA message, etc) in the IMS control data of the message
- Back end IMS can rebuild an ACEE for that user ID and use it for authorization
  - If further authorization is required on the back end

APPC

- User ID is in a control section of the input message

User ID Concepts (cont)

CICS (ISC)

- “Pooled connection”: messages from many users flow across the link
  - Unlike MSC, does not include control information for the user ID.
  - IMS treats it as a legacy terminal that signs on once with one user ID
- CICS itself can issue /SIGN ON
- CICS can define a default user ID
  - DFLTUSER
- If no sign on and no default user ID
  - dynamic links
    - USER ID=SUBPOOL name
  - static links
    - RACF uses IMS CTL user ID for transaction authorization
    - IMS puts LTERM name in user ID field of message

User ID Concepts (cont)

Messages from IMS Connect client => IMS Connect

- IMS Connect or IMS Connect client can do user ID verification

- RACF=Y/N in HWSCFG
  - RACF=Y ICON calls RACF to verify user ID and password
  - RACF=N ICON does not call RACF directly

- ICON User Message Exit
  - can do RACF user verification
  - can set “Trusted User” flag

User ID Concepts (cont)

From IMS Connect client => IMS Connect

- User ID and password or passticket in the message
  - Entered by IMS Connect client
  - Set by the IMS Connect User Message Exit

- APPLname is optional
  - Entered by IMS Connect client
  - Set by IMS Connect User Message Exit
  - Defaulted to on DATASTORE control cards

User ID Concepts (cont)

From IMS Connect => IMS OTMA

- ICON passes message with user ID or UTOKEN to IMS OTMA
  - ICON does not send password to IMS OTMA

- If OTMA security is active, OTMA calls RACF to build ACEE
  - OTMASE=C/F
  - OTMASE=P use the security specified in the message

- If RACF cannot build ACEE, message is rejected

- ACEE is cached by OTMA and can be “aged off” or “refreshed”

User ID Concepts (cont)

- If NMD BMP inserts a message
  - BMPUSID specifies what should be placed in user ID field of inserted message
    - BMPUSID=USERID is value of USER= on JOB statement
    - BMPUSID=PSBNAME
  - If BMPUSID is not specified the PSB is placed in the user ID field of the inserted message
  - Specify BMPUSID on the DFSDCxxx member of PROCLIB

- Message-driven BMP
  - Authorization is against the user ID associated with each transaction message
  - BMPUSID is ignored

User ID Concepts (cont)

- User ID is valid. What is the user authorized to do?

User ID Concepts (cont)

- When the user accesses a resource:
  - IMS calls RACF to check user's authorization to a resource
    - IMS passes ACEE to represent that user

    Example user submits ADDINV transaction:

    RACROUTE REQUEST=FASTAUTH,LOG=ASIS,
    ACEE=*nnnnnnnn*,CLASS=TIMS,ENTITY=ADDINV,ATTR=READ

  - If IMS doesn't have an ACEE for the user, IMS passes zero
    - RACF uses caller's "security environment"
    - Caller's security environment is CTL or MPR user ID

User ID Concepts (cont)

- Once a transaction is scheduled and running in MPR, what happens if it accesses another resource?
  - Issues CHNG call
  - Issues AUTH call
  - Does a deferred conversational program-program switch
  - Calls external subsystem (DB2, MQ)
  - Issues a command (AOI)
    - IMS commands are always processed in CTL
    - TRANSACT macro must specify AOI parameter

User ID Concepts (cont)

- Program does CHNG call, AUTH call, deferred conversational pgm switch
  - For non-OTMA, IMS dynamically builds a temporary ACEE in MPR
  - OTMA can access cached ACEE (no build necessary)
- Dynamically built ACEE does not change the MPR “security environment”

User ID Concepts (cont)

To avoid dynamic build

- DFSBSEX0 R15=04 builds ACEE in MPR when msg scheduled
- APPCSE=F builds ACEE in MPR when msg scheduled
- OTMASE=F builds ACEE in MPR when msg scheduled
- This changes the MPR “security environment”
  - MPR security environment is now end user ACEE

User ID Concepts (cont)

Be aware:

- If dynamic build fails
  - ACEE of caller's "security environment" is used
    - MPR user ID
    - CTL user ID

User ID Concepts (cont)

If the application program calls DB2

- IMS can pass user ID and group to DB2 Signon Exit
  - DB2 can do RACF VERIFY call
  - User ID passed is from original input message
    - Signed on user ID
    - LTERM if user not signed on
    - PSB or USER= if NMD BMP

or

- DB2 can access ACEE of MPR “security environment” directly
  - Enhancement PM27835

User ID Concepts (cont)

- DB2 can access ACEE of MPR “security environment” directly
  - MPR “security environment” is ACEE of MPR user ID
  - To set MPR security environment to ACEE of end user:
    - OTMASE=F
    - APPCSE=F
    - For non-OTMA non-APPC code DFSBSEX0 R15=04

User ID Concepts (cont)

Be aware:

- DFSBSEX0 Reg15=04 or OTMASE=F or APPCSE=F
  - Sets security environment of MPR = ACEE of user who submitted the message
  - **All** RACF calls for the message will use end user's ACEE
    - End user *may* need access to other resources like dump datasets, etc.

Solving User ID Problems

Now let’s solve some problems

Solving User ID Problems

Why does an active IMS user keep getting his user ID deleted from RACF?

- Last Access Date is not being updated.

- Only a VERIFY call will update the Last Access Date.
- For example: with MSC, if VERIFY call is done on the front end and the back end IMS uses a different RACF database, the user ID can look inactive on the back end RACF database.

Solving User ID Problems

Why are we seeing such high I/O to the RACF database coming from IMS?

- Do not always blame IMS.

- For example, if your DB2 Signon Exit specifies STAT=YES on the VERIFY, then every time DB2 does a VERIFY call, the user's profile is updated in the RACF database. You can specify STAT=NO or you can specify you only want stats updated once a day, or DB2 can access the existing ACEE that IMS has already verified.

Solving User ID Problems (cont)

My automation product is getting a security violation shutting down a WFI BMP.

- Your automation is using the WTOR to issue a transaction that tells the BMP to stop.
- RACF is called to authorize the transaction and a user ID is required.
- You can use WTORUSID to assign a user ID to the WTOR, define that user ID to RACF and give it authority to issue the transaction.
- Commands can be entered through WTOR without a sign on because RACF is not called for commands from WTOR.

Solving User ID Problems (cont)

Why did IMS Connect allow an unauthorized user to access a transaction even though I have RACF=Y?

- Because IMS Connect never does transaction authorization. RACF=Y tells IMS Connect to do user ID verification.
- IMS does the transaction authorization if you specify OTMASE=C/F/P

Solving User ID Problems (cont)

Why is DB2 returning -922 for users who should be authorized?

- Because when the transaction calls DB2, DB2 is directly accessing the ACEE of the MPR's "security environment".
- The MPR "security environment" is the MPR user ID and the MPR user ID is not authorized to the resources.

- You can change the "security environment" in the MPR by setting OTMASE=F for OTMA messages, APPCSE=F for APPC messages and DFSBSEX0 code 04 for all other messages.

Solving User ID Problems (cont)

We set OTMASE=F so DB2 can get the right user ID. Why is the MPR now getting security violations for LOGSTRM and JESSPOOL? The MPR is authorized to those resources.

- Because OTMASE=F tells IMS to build an ACEE for the end user in the MPR. This changes the "security environment" of the MPR to point to the end user's ID instead of the MPR's user ID. All RACF authorization calls while that user's transaction is processing will be made with that end user's ACEE.

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- **Exits**
- Dependent region security (RAS)
- References

Exit Concepts (cont)

- Can be used alone or with RACF
- May provide more granularity than the RACF profile
- Many exits can now be refreshed dynamically
- Can override the RACF result
  - Called after RACF

Exit Concepts (cont)

- If an exit cannot be explicitly specified, IMS will invoke it if it exists
  - The IVP may install sample exits into RESLIB if you specify RACF on IVP panel

- If an exit is explicitly specified, IMS will abend if it does not exist
  - U0718 on initialization

Exit Concepts (cont)

- The Command Authorization Exit (DFSCCMD0) is not invoked by Operations Manager (OM)
  - OM invokes its own user exits
- The Transaction Authorization Exit (DFSCTRN0) is never invoked if the RACF return code is greater than 4.
- The Transaction Reverification Exit (DFSCTSE0) is invoked if the RACF return code is greater than 4

Exit Concepts (cont)

- The Build Security Environment (DFSBSEX0) is invoked before the message is given to the application program
  - Not initially called for messages from OTMA, APPC, NMD BMP

- DFSBSEX0 is always invoked for CHNG and AUTH calls no matter where the original message came from

- DFSBSEX0 is called when the security environment does not exist
  - For example: CHNG call on back-end SMQ or MSC

Exit Concepts (cont)

- With IMS13 exits no longer linked into Nucleus
  - Sign On DFSCSGN0
  - Transaction Authorization (DFSCTRN0)
  - Transaction Reverification (DFSCTSE0)
- With IMS13 these exits are:
  - standalone members of RESLIB
  - invoked if they exist
  - loaded dynamically
    - use of VCONs to reference other modules or ctl blks will no longer work
- New initialization call (R0=4) added for DFSCSGN0
  - verify your DFSCSGN0 exits will function correctly with this new entry vector

Solving Exit Problems

Now let’s solve some problems

Solving Exit Problems (cont)

RACF rejected the command but IMS did it anyway!

```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA ) GROUP(IMSOPRL ) NAME(#####
              785 00000281    ASS CL(CIMS    )
              785 00000281    INSUFFICIENT ACCESS AUTHORITY
              785 00000281    ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )

DFS058I 15:36:21 ASSIGN COMMAND COMPLETED
```

Command Authorization Exit (DFSCCMD0) allowed the command.

Solving Exit Problems (cont)

Results when DFSCCMD0 was removed from RESLIB:

```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA ) GROUP(IMSOPRL ) NAME(#####
              785 00000281    ASS CL(CIMS    )
              785 00000281    INSUFFICIENT ACCESS AUTHORITY
              785 00000281    ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )

DFS3662W 16:23:58 COMMAND REJECTED BY RACF; USER NOT AUTH   ; RC= 0008
```

Solving Exit Problems (cont)

I removed the sample DFSCCMD0 exit from RESLIB and now IMS won't come up.

- Because any of these parameters cause IMS to load DFSCCMD0
  - CMDSEC=E or A
  - AOI1=A or C
  - AOIS=A or C
  - CMDMCS=B or C

- **Any** exit you explicitly specify must exist or IMS will abend.
  - U0718

Solving Exit Problems (cont)

After migrating to IMS13, we started getting sign on security violations

- Because there was an old version of DFSCSGN0 exit in RESLIB
- Prior to IMS13, it was not invoked because SECURITY macro specified NOSIGNEXIT
- IMS13 invokes it because it is in RESLIB

Solving Exit Problems (cont)

- Are there exits in your RESLIB?
  - Should they be there?
  - Are they old?
  - Do you want them?
  - When IMS comes up, look for
    DFS1937I USER EXIT DFSxxxx0 LOADED


Maybe they won't notice
MSKU 524 478 8
22G1
POLICE
BRD 204 B

Areas We Will Explore

- Security Activation
- RACF resource class and profile
- User ID
- Exits
- **Dependent region security (RAS)**
- References

The APPL Gate

RAS Concepts (cont)

RACF APPL class

- Restrict terminal users' access to applications (TSO, IMS, CICS, etc.)
  - Define a RACF profile for *sapplid* in APPL class
  - Specify *sapplid* in DFSDCxxx
  - *sapplid* defaults to *imsid*

- Control ATTACH requests
  - Protect conversations between partner LUs

- Control whether a dependent region can connect to IMS
  - **This check is only made if IMS RAS security is active (ISIS=R|A)**
  - Examples of dependent regions: BMP, CICS, DB2 stored procedure
  - Define a RACF profile for *imsid* in the APPL class

RAS Concepts (cont)

With RAS enabled (ISIS in DFSPBxxx):

- First RAS check: getting through the gate
  - Is the dependent region allowed to connect to IMS
  - Protect imsid in RACF APPL class
  - If RAS security is activated ***all*** authorized dependent regions need access
    - PERMIT IMSP CLASS(APPL) ID(MPP1,BMP1,CICS1,etc.) ACCESS(READ)
  - The RAS exit DFSRAS00 can specify exclusions from this check.

RAS Concepts (cont)

With RAS enabled (ISIS)

- Second check: getting in the house
  - Is the dependent region allowed to access PSB, TRAN, LTERM?
  - Define resources you want to protect
    - IIMS/JIMS for PSB
    - TIMS/GIMS for TRAN
    - LIMS/MIMS for LTERM
  - If RAS security is activated ***all*** authorized dependent regions need access to the resources
  - The RAS exit (DFSRAS00) can define exclusions from these checks

Solving RAS Problems

Now let’s solve some RAS problems

Solving RAS Problems (cont)

An unauthorized user updated a production database!

- Because the user submitted a BMP and ISIS=N
- Without RAS security
  - Any user can submit a BMP from TSO for any PSB with no security checks
- Some customers use alternative controls for job submission
  - RACF Program Control
  - job scheduling product
  - z/OS exit

Solving RAS Problems (cont)

I activated RAS and now my MPRs won't come up.

DFS2854A …. FAILED SECURITY CHECK

- Because with RAS active, all dependent regions need access to the imsid and any protected resources accessed in that region
  - The user ID of the MPR must be authorized to imsid
  - The user ID of the MPR must be authorized to transactions
  - DFSRAS00 exit can be used to bypass the MPR security check

Solving RAS Problems (cont)

I added a new transaction and gave the users access to it. Why are they getting RACF violations?

- The message region is getting the violation, not the user. RAS is active and you did not give the MPR access to the transaction.
  - You will see that the user ID specified in the ICH408I message is the MPR, not the user who submitted the transaction.
- The user ID of the MPR must be authorized to transactions
- DFSRAS00 exit can be used to bypass some checking

Solving RAS Problems (cont)

- You can use the RAS exit (DFSRAS00) to bypass security checks for certain regions, resources, region types, etc.
  - For example you could activate RAS only for BMPs

Solving RAS Problems (cont)

It's too much work to protect the imsid because I will have to define all the online users in the RACF access list for the imsid.

- You can define a value for SAPPLID that is different from the imsid and leave that access open.
  - RACF VERIFY for online users is always done against SAPPLID
  - RACF VERIFY for dependent regions is always done against IMSID
  - SAPPLID (in DFSDCxxx) defaults to IMSID

- Using SAPPLID also allows you to separate access
  - For example: let a user sign onto IMS but not submit BMPs

REFERENCES

References

- IMS Home Page

  www.ibm.com/ims contains links to

  - Upcoming Webcasts, Roadshows and other events
  - Samples submitted by IBM and customers (IMS Examples Exchange)
  - Presentations/papers
  - Library
  - IMS Tools and the Tools library
  - Information Center
  - IMS Newsletters
  - And more

References (cont)

User Groups and Forums

IMS Regional User Groups
www.ims-ug.org

IMS-L
http://imslistserv.bmc.com/

Virtual IMS Connection
http://www.virtualims.com

References (cont)

New 3-volume Redbook set for Security on the IBM Mainframe

Volume 1 published December 2014. Volume 2 and 3 in the future.

Security on the IBM Mainframe, Vol. 1 A Holistic Approach by Reducing Risk and Improving Security SG24-7803-01

Vol 1: Overall introduction of mainframe security architecture and best practices

Vol 2: Networking and communications server security architecture and best practices

Vol 3: Security architecture and best practices for software products like DB2, CICS, IMS

References (cont)

IBM strongly suggests that all System z customers be subscribed to the IBM System z Security Portal to receive the latest critical System z security and system integrity service. If you are not subscribed, see the instructions on the System z Security web site

http://www-03.ibm.com/systems/z/advantages/security/integrity_sub.html

Security and system integrity APARs and associated fixes will be posted to this portal. IBM suggests reviewing the CVSS scores and applying all security or integrity fixes as soon as possible to minimize any potential risk.

The “windows”	The keys	Where to find the keys
3270 terminal	RCF	DFSPB
TCO script	RCF and TCORACF	DFSPB
OTMA	OTMASE	DFSPB
ODBA	ODBASE or ISIS	DFSPB
APPC / LU 6.2	APPCSE	DFSPB
MSC	MSCSEC	DFSDC
Operations Manager (OM)	CMDSEC	CSLOI DFSCG or DFSDF
MCS or E-MCS	CMDMCS	DFSPB
DBRC	CMDAUTH	RECON
AOI type 1	AOI1	DFSPB
AOI type 2	AOIS	DFSPB
Dependent region	ISIS	DFSPB

IMS General Resource Profiles

IMS resource	Resource class singular/grouping	Resource name
Transaction	T*IMS* / G*IMS*	transaction code
Command (type 1)	C*IMS* / D*IMS*	first 3 characters of command
DBRC command	FACILITY	*safhlq*.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.*plxname*.command_verb.command_keyword
Program (PSB)	I*IMS* / J*IMS*	program name
Logical terminal	L*IMS* / M*IMS*	logical terminal name (lterm)
CF structure	FACILITY	CQSSTR.*structure_name* or IXLSTR.*structure_name*
IMS Control Region	APPL	*imsid*
IMSPlex (CSL)	FACILITY	CSL.*imsplexname*
XCF group (Client bid)	FACILITY	IMSXCF.groupname.*membername*
Dataset	DATASET	*dataset name*

RLIST CIMS DBR AUTHUSER

```
CLASS      NAME
 -----      ----
 CIMS       DBR

 GROUP CLASS NAME
 -----  -----  ----
 DIMS

UNIVERSAL ACCESS
 -----
NONE

USER       ACCESS
 ----       ------
SYSPROG    READ
 DBA01      READ
 SUZIE      READ
```

RLIST TIMS TRAN AUTHUSER*

```
CLASS      NAME
 -----      ----
 TIMS       TRAN21*    (G)

 GROUP CLASS NAME
 -----      -----      ----
 GIMS

UNIVERSAL ACCESS
 -----
READ

USER      ACCESS
 ----       ------
HENRY      NONE
```

*RLIST GIMS * AUTHUSER*

```
      CLASS      NAME
 GIMS             TRAN2NNN

 MEMBER CLASS NAME
 -----        -----      ----
 TIMS

RESOURCES IN GROUP
--------- -- -----
TRAN2*  (G)
ADDINV

UNIVERSAL ACCESS
 -----
NONE

USER         ACCESS
 ----          ------
USER200      READ
```

Write to me!

Maida Snapper

maidalee@us.ibm.com