Secrets of IMS Security

Did You Lock Up?

October 23, 2012
Maida Snapper
maidalee@us.ibm.com
845-620-5762

Disclaimer

Agenda

What is IMS?

What IMS resources can RACF protect?

How do you lock the gate, the doors and the windows with RACF?

How do you set up RACF definitions for IMS?

Who (or what!) are the users of IMS?

When and how does IMS talk to RACF?

How can you tell if IMS is secure?

What is IMS?

What is IMS?

DATABASE Manager

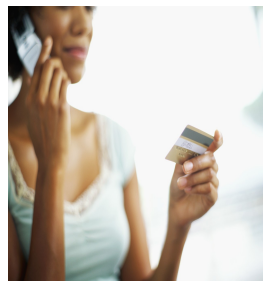
and

TRANSACTION Manager

The World Depends on IMS

IMS is a part of everyday life……..


ATM




FRAGILE

How can you protect these important business functions?

Security Facilities IMS Can Use

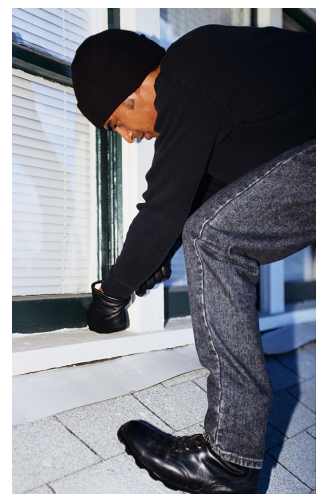
- **RACF (or other SAF product)**
- Encryption
- IMS default security
- Program Specification Block (PSB)
- VSAM password protection
- Application-based security
- Physical security
- IMS Exits

IMS Resources RACF Can Protect

- IMS itself
- Commands
- Transactions
- Datasets
- Databases
  - records, segments, fields
- Programs (PSBs)
- Terminals (Logical, Physical)
- Coupling Facility Structures
- IMSPlex and XCF group membership

How are they trying to get in?

There's an IMS lock for that.



IMS Windows and Doors: How IMS Messages Get In

SNA Terminal (static or ETO)
System Console (WTOR)
IMS Master terminal
MCS or E-MCS device
OTMA (IMS Connect, MQ, etc)
ODBA (DB2 stored procedure, distributed environment)
Operations Manager
APPC/LU6.2
MSC link
ISC link (LU6.1)
TCO script
DBRC utility
Dependent region (BMP, CICS, etc.)
AOI program

First Line of Defense: Lock the Gate

Can you prevent a user from signing on to IMS?

Can you prevent a user from submitting an IMS job?

Yes!

The APPL Gate

RACF APPL Class

RACF APPL class

- Restrict terminal users' access to applications (TSO, IMS, CICS, etc.)

- Control ATTACH requests
  - Protect conversations between partner LUs

- Control which dependent regions can connect to IMS
  - Check only made if RAS security is active (ISIS=R|A)
  - Examples of dependent regions: BMP, CICS, DB2 stored procedure

RACF APPL Class (continued)

- Define profile(s) for the IMS control region
  - Profile name *imsid*
    - For dependent regions and attach requests
  - Profile name *sapplid*
    - For terminal users

- When a **person** signs on to IMS
  - Request to sign on to *sapplid*
    - RACROUTE REQUEST=VERIFY,APPL=*sapplid*
    - *sapplid defaults to imsid*
  - *User IDs or groups need READ*

- When a **dependent region** (BMP, CICS, etc.) "signs on" to IMS
  - Request to connect to APPL=*imsid*
  - If IMS RAS security is active, all dependent region user IDs or groups need READ

How do you set up the RACF definitions for IMS users and resources?

Setting Up RACF

- Define Resource Classes in Class Descriptor Table (CDT)
- Activate Resource Classes
  - CLASSACT
- Populate the RACF database
  - Add group & user profiles
    - ADDUSER
    - ADDGROUP
  - Connect users to groups
    - CONNECT
  - Define resource profiles
    - RDEFINE
  - Create access lists
    - PERMIT

A resource is identified by

Resource Class + Resource Name

IMS Resource Classes

Default IMS RACF General Resource Classes

RACF default resource classes used exclusively by IMS (RCLASS=IMS)

CIMS | DIMS	**Commands**
TIMS | GIMS	**Transactions**
IIMS | JIMS	**Application programs (PSBs)**
LIMS | MIMS	**Logical terminals (LTERM)**
AIMS	APSB (Allocate PSB) for CPIC-PSB and ODBA
RIMS	Asynchronous hold queues for RESUME TPIPE call
PIMS | QIMS	Databases (for AUTH call)
FIMS | HIMS	Database fields (for AUTH calls)
SIMS | UIMS	Database segments (for AUTH calls)
OIMS | WIMS	Other (information in RACF for AUTH calls)

RACF General Resource Classes

These RACF resource classes are also used by IMS

TERMINAL | GTERMINL
APPL
DATASET
FACILITY
OPERCMDS
STARTED
VTAMAPPL
APPCPORT
APPCLU
APPCTP

If your RACF database is shared,

can IMS systems

have different security rules

for the same resources
?

Yes!

Because a resource is identified by

Resource Class + Resource Name

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*

IMS points to its own set of security rules

using the IMS RCLASS parameter

RCLASS = position 2-8 of the resource class

Default RACF Resource Classes

RCLASS defaults to ***IMS*** when not specified

T*IMS*
G*IMS*

C*IMS*
D*IMS*

I*IMS*
J*IMS*

L*IMS*
M*IMS*

transactions

commands

programs

logical terminals

Sample Installation-defined RACF Resource Classes

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

T*IMSTEST*
G*IMSTEST*

C*IMSTEST*
D*IMSTEST*

I*IMSTEST*
J*IMSTEST*

L*IMSTEST*
M*IMSTEST*

transactions

commands

programs

logical terminals

Defining a New IMS RACF Resource Class

- Class name 1-8 alphanumeric characters
  - First character must be the same as its corresponding default class:
    - C, D, T, G, I, J, L, M, A, R, etc.

- You must define both the singular and its grouping class.

- **Model new classes on the corresponding default class**
  - Optionally can change the POSIT value
  - Do not change MAXLNGTH

- Activate new resource classes
  SETR CLASSACT(*classname*)

RACF Resource Class

- Class Descriptor Table (CDT)
  - entries can be defined statically (IPL) or dynamically (no IPL)
  - maximum 1024 entries
    - 256 default classes delivered with RACF
    - 768 can be installation-defined
  - loaded at IPL by merging static, then dynamic class descriptors
    - dynamic entry replaces static of the same name
    - if merge reaches 1024, RACF warns entries are being ignored
  - CDT processes a paired member and grouping class together.

- There is no need to update the RACF Routing Table
  - ACTION=RACF is the default

Supplied CDT entries are documented in Appendix C of the z/OS Security Server RACF Macros and Interfaces

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

Secret: Bigger is not better

If you define a new IMS resource class,

use the same MAXLNGTH

as the corresponding default IMS resource class.

POSIT Values

You can specify POSIT values 19–56 and 128–527.

POSIT values 0–18, 57–127, and 528–1023 are reserved for IBM use and should not be used for your installation-defined class entries unless you intend to share SETROPTS options with an IBM supplied class.

Secret: ***If a required class is inactive, IMS will abend.***

Define ***and*** **Activate** classes or IMS may abend U0166

Example: to activate CIMS
(and all other classes with the same POSIT value as CIMS):

SETROPTS CLASSACT(CIMS)

Profiles

RACF Profiles

- **Group** profile
  Defines group name, group authority, subgroup, ...

- **User** profile
  Defines individual user ID, password, user attributes, connect groups, ...

- **Resource** profile
  Defines Universal Access and authorized users (access list)
  - Discrete
  - Generic
  - Fully Qualified Generic

GROUP and USER Profiles

Who/what are IMS users?

Why do they sometimes have strange user IDs that don't conform to your installation standards?

Secret: An IMS User Isn't Always a Person

A user ID can represent a...

- Person
- Job, Started Task (BMP, utility, etc.)
- Transaction
- Command
- Logical terminal (LTERM, Master, WTOR, TCO)
- Program (PSB)

Example of an IMS Transaction Acting as a "User"

A programmer writes a program that issues an IMS command.
When the program runs, RACF checks to see if the program is authorized to issue the command. RACF needs a user ID.

The three choices for user ID in this case are:

1) User ID of the person who entered the transaction that invoked the program
   - Resource is the command
   - **This choice allows the person to also enter the IMS command directly**

2) User ID is the transaction code
   - Resource is the command
   - Recommend NOPASSWORD
     - IMS calls RACF to VERIFY the ID with PASSCHK=NO

3) User ID is the command
   - Resource is the transaction code
   - Recommend NOPASSWORD and RESTRICTED
     - IMS calls RACF to VERIFY the ID with PASSCHK=NO

Access Lists

RACF Access Authority

- User or Group Access Authority (ACCESS) can be:
  - NONE
  - EXECUTE
  - READ
  - UPDATE
  - CONTROL
  - ALTER

- Maximum entries in the access list of a profile is 5957
  - access list of each profile is limited to 65535 bytes
  - each user or group in the access list uses 11 bytes

- **READ is sufficient for most IMS general resources**

- UPDATE is required for some IMS general resources
  - Some Type 2 commands
  - CQS access to CF structures (SMQ and RM)
  - Registering with SCI to join an IMSplex

RACF Access Authority for the RECON dataset

- READ is sufficient for readers
  - they must specify the READONLY parameter
- UPDATE is sufficient for all accesses except DELETE and DEFINE
- ALTER required for DELETE and DEFINE
- CONTROL is never required anymore

Secret: RECONs Come in Sets of Three

- Each IMS has 3 RECON datasets
- Each of the 3 RECON datasets might have a different high level qualifier
- Users must have the same RACF access to all 3 RECON datasets
  - If VSAM open gets RACF violation, IMS discards the RECON

- ADDSD ('PROD1.RECON1', 'PROD2.RECON2', 'PROD3.RECON3') UACC(NONE)

How much authority does IMS itself need?

- IMS needs access to its datasets
  - JCL defined
  - Dynamically allocated
- IMS does not normally need to access transactions or commands
  - If a user ID is not available, RACF uses the IMS user ID for authorization
- IMS does not need to be defined as privileged or trusted

What happens if there is conflicting information in the RACF database?

RACF uses

the most restrictive UACC

the most permissive ACCESS

Secret: Undefined IMS resources are authorized

What happens if the resource is not defined to RACF?

IMS allows access.

RACF sends a return code of 4 when a resource is not defined to RACF

IMS treats return code 4 and return code 0 the same.

Making RACF Changes

- To update RACF security definition
  - update the RACF database
  - refresh the RACF data space from the database by issuing
    SETROPTS RACLIST(*classname*) REFRESH
- RACF refreshes all classes with the same CDT POSIT value as *classname*
- specify the *member* classname not the grouping classname
  for example, specify CIMS not DIMS
- REFRESH must be entered on all members of a SYSPLEX unless RACF is configured for SYSPLEX communication

You added a profile to RACF to protect the /STA command with UACC(NONE).

Why can everyone still issue /STA?

Did you REFRESH ?

Refresh the RACF Dataspace(s)

- Updating a RACF resource profile updates the RACF *database*.
- REFRESH the RACF *dataspace* for the update to take effect.

For example
SETR RACLIST CLASS(CIMS) REFRESH
SETR GENERIC (CIMS) REFRESH

This brings in a new copy of all profiles in the CIMS class.
It also refreshes any other classes with the same POSIT value as CIMS.

Recycling IMS does not refresh IMS resource definitions in the RACF dataspace.

Secret: You rarely have to recycle IMS for RACF changes

Two rare cases when IMS has to be recycled for a RACF change to take effect:

1) For DATASET resource: if new access is given to a GROUP and IMS was not previously connected to that GROUP you have to recycle IMS.

2) For general resource: if you activate a new IMS class you have to recycle IMS to get it loaded into a RACF dataspace

How and when does IMS talk to RACF?

The SAF Interface

- IMS calls RACF through the SAF interface
  - RACROUTE call

- RACF builds Accessor Environment Element (**ACEE**) for each signed on user
  - Constructed by RACF when user signs on
  - Deleted when user signs off
  - Contains a description of the user's security environment

z/OS Security Server RACF RACROUTE Macro Reference
z/OS Security Server RACF Data Areas (for description of ACEE)

When IMS Comes Up and Initializes

- IMS calls RACF to load general resource profiles into data spaces
  (DATASET, Group, User profiles not eligible)

  RACROUTE REQUEST=**LIST**,GLOBAL=YES

- RACF builds ACEEs for IMS user ID (and DL/I, DBRC)

.

When A User Signs On

- IMS calls RACF for user ID verification

```
RACROUTE REQUEST=VERIFY,
                ENVIR=CREATE
                USERID=
                GROUP=
                PASSCHK=YES/NO
                PASSWRD=
                APPL=sapplid
                TERMID=
                ACEE=addr…..
```

- RACF verifies user ID, password, group, physical terminal, **application**
- RACF builds ACEE
- RACF returns ACEE address and SAF return code to IMS
- IMS logs x'16'

When A Dependent Region Connects to IMS

- IMS calls RACF for user ID verification **only if IMS RAS security is active**

```
RACROUTE REQUEST=VERIFY,
                 ENVIR=CREATE
                 USERID=
                 GROUP=
                 PASSCHK=YES/NO
                 PASSWRD=
                 APPL=imsid
                 TERMID=
                 ACEE=addr…..
```

- RACF verifies user ID, password, group, physical terminal, **application**
- RACF builds ACEE
- RACF returns ACEE address and SAF return code to IMS
- IMS logs x'16'

When A Resource Is Accessed

- IMS calls RACF to check authorization
  IMS passes ACEE, CLASS, ENTITY, ATTR

  Example:
  RACROUTE REQUEST=**FASTAUTH**,LOG=ASIS,
  ACEE=addr,
  CLASS=CIMS,
  ENTITY=DIS,
  ATTR=READ

- RACF sends SAF return code to IMS
  - 0 user is authorized, IMS grants access
  - 4 resource has no profile, **IMS grants access**
  - 8 user is not authorized
    - IMS denies access and logs x'10'
    - RACF issues ICH408I message and logs SMF TYPE 80

If A User Is Not Signed On

- If a USER ID is not available, IMS passes zeroes in the ACEE field.
- IMS calls RACF to check authorization

  Example:

  RACROUTE REQUEST=FASTAUTH,LOG=ASIS,

  ACEE=00000000,CLASS=CIMS,ENTITY=DIS,ATTR=READ
- RACF uses the ACEE of the “home” address space

  usually home is IMS control region

  in some cases home is dependent region

When A User Signs Off

- IMS calls RACF to delete the user's ACEE

  RACROUTE REQUEST=**VERIFY**,ENVIR=DELETE,ACEE=addr…

- IMS logs x'16'

When IMS Shuts Down

- IMS calls RACF to deregister interest in the resource classes

  ..

- RACF deletes the ACEE for IMS user ID

- **GLOBAL=YES data spaces are not deleted**

Summary: IMS Calls RACF when…….

- When IMS comes up:
  - RACLIST
- When user signs on
  - VERIFY (CREATE)
- If IMS RAS security is active, when dependent region connects
  - VERIFY (CREATE)
- When user accesses a resource
  - FASTAUTH, AUTH
- When user signs off
  - VERIFY (DELETE)
- When IMS comes down

Each "Window" Has a Lock

How is the message getting in ?	*What is the IMS lock?*	*Where is the IMS lock?*
SNA Terminal (static or ETO)	RCF	DFSPBxxx
TCO script (special case of static terminal)	TCORACF and RCF	DFSPBxxx
MCS or E-MCS console	CMDMCS	DFSPBxxx
Dependent region (MPP,BMP,CICS, etc.)	ISIS	DFSPBxxx
AOI program (tran issues CMD call)	AOI1	DFSPBxxx
AOI program (tran issues ICMD call)	AOIS	DFSPBxxx
DBRC	CMDAUTH	RECON
OTMA (ex. IMS Connect, MQ)	OTMASE	DFSPBxxx
ODBA (ex. DB2 stored procedure)	ODBASE	DFSPBxxx
Operations Manager (OM)	CMDSEC	CSLOIxxx DFSCGxxx
APPC/LU6.2	APPCSE	DFSPBxxx
MSC link	MSCSEC	DFSDCxxx

A programmer with ***no access*** to production,

accidentally updated production data!!!!!!!

How can this happen?

Secret: ***The dependent region window might be unlocked.***

How did the user access IMS?

User submitted a BMP from TSO

Dependent region “window” was not locked.
ISIS=N

You gave everyone access to the IMS DISPLAY command

RDEF CIMS DIS UACC(READ)

Why can’t some people do /DIS?

Secret: IMS provides some default command protection

How did the user access IMS?
OTMA client

The OTMA “window” was not locked
OTMASE=N

Since no security was specified for OTMA, default command security was in effect.

Commands allowed by default when OTMA is the source of command entry:

/LOCK /LOG /RDISPLAY

RACF rejected a command but IMS did it anyway!

Why?

Secret: IMS Exits Can Override RACF

```
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
```

RACF rejected the command.

The IMS Command Authorization Exit gets control after RACF and can allow the command.

IMS Exits Can Override RACF

Results when the IMS exit was removed or changed:

```
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
```

Secret: There Are Database Copies, Back-Ups, Logs

Don't forget to protect these too:

- Back-up copies (“Image Copy”) of databases on tape or disk

- Archived logs on tape or disk

How can you tell if IMS is secured?

Determining the Security in Effect

The security in effect for a given input message is determined by ...

- IMS system definition (IMSGEN)
- IMS JCL overrides
- IMS PROCLIB overrides
  - DFSPBxxx
  - DFSDCxxx
  - CSLOIxxx
  - DFSCGxxx
- IMS commands and restart options
  - Example: /SECURE APPC FULL
- Source of the input message
- RACF definitions
- Exits
- Program Specification Block (PSB)
- Database Definition Block (DBD) - encryption

Summary

What is IMS?

What IMS resources can RACF protect?

How do you lock the IMS doors and windows with RACF?

How do you set up RACF definitions for IMS?

Who (or what!) are the users of IMS?

When and how does IMS talk to RACF?

How can you tell if IMS is secure?

Call or Write

Maida Snapper
maidalee@us.ibm.com
845-620-5762