IBM Software Group

IMS16 IMS/SMU Security Converting to RACF with IMS Version 9

Richard Schneider
IMS developer
riccis@us.ibm.com

Overview

- ***IMS Version 9 will be the last release of IMS to support SMU***
- **Version 9 introduces new RACF* facilities**
  - **All SMU usage can now be replaced with RACF security**

This presentation:

- **Considers the SMU facilities that previously had no directly corresponding RACF facilities**
- **Explains the corresponding RACF options in Version 9**

* In this presentation, “RACF” should be interpreted as “RACF or equivalent product”

RACF Security Before IMS Version 9

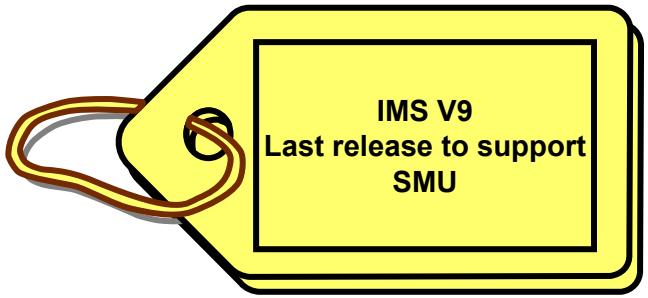
Most IMS security can already be implemented with RACF

- **Sign-On user validation and verification**
  - Check user is known
  - Check password is correct
- **Terminal Security**
  - User v. physical terminal
- **IMS System Access Security**
  - User v. IMS ID
- **Transaction Security**
  - User v. Trancode
- **Command Security**
  - User v. IMS Command in Control Region
  - User v. IMS Command in Operations Manager
- **AOI Type2 ICMD Call Security**
  - User v. IMS Command
- **IMS Data Set Access Security**
  - Controls access to DBs and system datasets
- **DB Data Access Security – used with DL/1 AUTH call**
  - User v. DB Record
  - User v. Segment
  - User v. Field
- **PSB Access Security - For ODBA and CPI-C**
  - User v. PSBname
- **Connection Access Control**
  - IMS Connect, CQS, CSL address spaces, etc

Security Enhancements in IMS V9

- **Version 9 introduces enhancements to the RACF interface to support:**

1. **Application Group Name (AGN) security**
2. **Type 1 and Type 2 Automated Operator Interface (AOI)**
3. **Terminal security for Time-Controlled Operations (TCO)**
4. **MSC link receive security**
5. **/LOCK, /UNLOCK and /SET commands**
6. **Signon verification**



- **Benefits**
  - Overcomes limitations that previously prevented migration from SMU

Resource Access Security

(Replaces AGN Security)

Resource Access Security with SMU

- **Uses Application Group Name (AGN) security**
  - IMS Version 9 is the last release to support AGN security
- **Objectives of AGN Security**
  - Check at Program Scheduling Time that the resources involved (PSB &/or TRANcode &/or LTERM) are authorised to be used by the Dependent Region
- **Predominantly used for BMPs, but actually applies for all dependent regions and connecting threads (DRA/CCTL/ODBA)**

AGN Security Requirements

- **THREE Required Elements**

1. AGN defined in SMU
   - A named group of
   - PSBs &/or Transaction Codes &/or LTERMnames

2. RACF (optional – can alternatively use DFSISIS0 Exit)
   - Define AGN in AIMS resource class
   - Permit userids to use AGN

3. Dependent Region JCL must contain AGN=xxx execution parameter
   - Would also contain USERID

AGN Security Checks

- **At Dependent Region Startup**
  - AGN name (**if** specified in JCL) is authorised for use by **Region's USERID**
    - RACF or DFSISIS0 (Resource Access Security Exit)

Mostly, in practice, AGN security is only used with BMPs

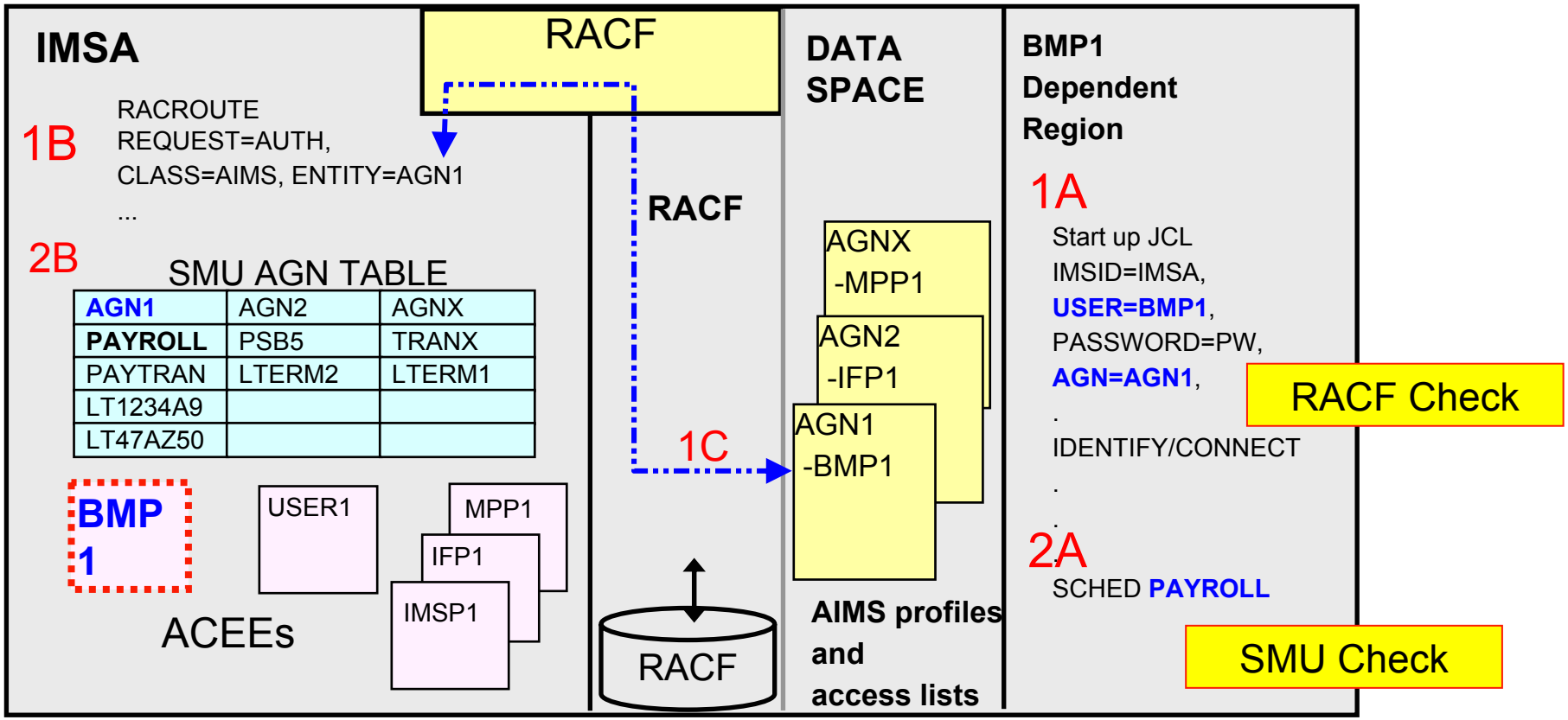
- **At Program Scheduling Time**
  - Check (performed by SMU) that required IMS resource(s) are in the AGN group for this region
    - MPP / JMP : check TRAN in AGN*
    - Message Driven BMP : check TRAN and PSB in AGN*
    - NMD-BMP / IFP / JBP : check PSB in AGN
    - NMD-BMP with OUT= : additionally check output LTERM / TRAN in AGN

* If LTERMs are included in AGN for a message driven region, then use of the region will be limited to LTERMs in the group

Resource Access Security (RAS)

- **The old way - SMU and AGN ...**

BMP Example – Relies on "AGN=" being coded in JCL



An alternative to the use of RACF is the use of the DFSISIS0 exit – renamed to "AGN Security Exit" (one or the other is called, not both)

Resource Access Security (RAS) with IMS V9

- **The new way in IMS V9**

  - Provides direct RACF authorization checking at program scheduling time of ***Region Userid*** against *IMS Resource* (TRAN, PSB, LTERM)

  - Uses new RACF security classes for PSBs and LTERMs
    - IIMS: Program Specification Block (PSB)
    - JIMS: Grouping class for PSB
    - LIMS: Logical terminal (LTERM)
    - MIMS: Grouping class for LTERM

  - Uses existing RACF security classes for Transactions
    - TIMS: Transaction (TRAN)
    - GIMS: Grouping class for Transactions

PSBs in AIMS class are for ODBA and Explicit APPC use of APSB only

(further details will follow)

Enabling Resource Access Security in IMS V9

- **New specifications in system definition**
  - **SECURITY** ... TYPE = **RASRACF | RASEXIT | RAS | NORAS |**
    | NOAGN | RACFAGN | AGNEXIT

RASRACF = RAS security invokes RACF
RASEXIT = RAS security invokes an IMS user exit (DFSRAS00)
RAS = RAS security invokes RACF and user exit DFSRAS00
NORAS = No security (turns off both RAS and SMU)

- **New specifications during startup (DFSPBxxx exec parameter)**
  - **ISIS** = **N | R | C | A** | 0 | 1 | 2

N = No security (turns off both RAS and SMU)
R = RAS security invokes RACF
C = RAS security invokes an IMS user exit (DFSRAS00)
A = RAS securityinvokes RACF and user exit DFSRAS00

defaults to SECURITY ... TYPE= specification

- ISIS =N | 0 turn off both RAS and SMU security checking

Resource Access Security Checks

- **New user exit (DFSRAS00) is called <u>after</u> RACF (when both are used)**
  - Provides authorization of IMS resources to IMS dependent regions in a RAS environment

- **RACF and/or DFSRAS00 make checks at scheduling time <u>using Region's USERID</u>**
  - Authorize region against transaction (MPP, JMP)*
  - Authorize region against PSB (IFP, NMD BMP, JBP, DRA|CCTL|ODBA)
  - Authorize region against transaction and PSB (MD BMP)*
  - Authorize region against PSB and OUT=LTERM (NMD BMP, JBP)
  - Authorize region against PSB and OUT=transaction (NMD BMP, JBP)

    * Also check region userid can use LTERM (if LTERM defined in LIMS class)

- **Available in DCCTL, DB/DC, and DBCTL**
  - DFSISIS0 remains available in an AGN environment for V9, but AGN security and the new RAS security can not coexist in a single IMS system

Resource Access Security and APSB Security

- **When RAS is enabled**
  - RAS check is made at every MPP/JMP program schedule using region's userid
  - RAS check is made at every BMP/IFP/JBP program schedule using region's userid
  - RAS check is made at every CICS/DBCTL program schedule using userid of CICS address space
    - Completely separately, CICS can perform check of terminal user against PSB
- **RAS checking takes place at a program schedule**
  - PSB defined in IIMS RACF class

  APSB security checking takes place for an "APSB Call"
  - PSB defined in AIMS RACF class

    IMS will never use both checks for the same schedule!
- **ODBA APSB call**
  - Exec parameter "ODBASE=Y" means use APSB security
  - With ODBASE=N, RAS (or AGN) security will apply (if enabled)
- **Explicit APPC (CPI-C) APSB call**
  - If APSB security is performed (with caller's userid), RAS check will not be made
  - If APSB security is not performed, RAS check (if enabled) will be performed using region's userid

RAS Migration Examples

Example 1 - BMP with OUT=lterm/tran

OLD

AGN definitions:

```
)( AGN  IMSDGRP
   AGPSB   DEBS
   AGPSB   APOL1
   AGTRAN TRANA
   AGTRAN TRANB
   AGLTERM IMSUS02
   AGLTERM T3270LD
```

RACF definitions
(userid to AGN group):

```
ADDUSER BMPUSER1

RDEFINE AIMS IMSDGRP OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSDGRP CLASS(AIMS) ID(BMPUSER1) ACCESS(READ)
SETROPTS CLASSACT(AIMS)
```

NEW

RACF definitions:

```
ADDUSER BMPUSER1

RDEFINE JIMS RASPGRP  ADDMEM(DEBS,APOL1) UACC(NONE)
PERMIT RASPGRP CLASS(JIMS) ID(BMPUSER1) ACCESS(READ)
RDEFINE GIMS RASTGRP ADDMEM(TRANA,TRANB) UACC(NONE)
PERMIT RASTGRP CLASS(GIMS) ID(BMPUSER1) ACCESS(READ)
RDEFINE MIMS RASLGRP  ADDMEM(IMSUS02,T3270LD) UACC(NONE)
PERMIT RASLGRP CLASS(MIMS) ID(BMPUSER1) ACCESS(READ)
```

RAS Migration Examples ...

Example 2 - AGN name with access to all entities of a particular resource type

OLD

AGN definitions:

```
)( AGN  ALLGRP
     AGPSB  ALL
     AGTRAN  ALL
```

In RACF, generic resource definitions can be used

NEW

RACF definitions:

```
ADDUSER DRAINBMP

RDEFINE JIMS ** UACC(NONE)
PERMIT ** CLASS(JIMS) ID(DRAINBMP) ACCESS(READ)
RDEFINE TIMS ** UACC(NONE)
PERMIT ** CLASS(TIMS) ID(DRAINBMP) ACCESS(READ)
```

Migrating Off SMU

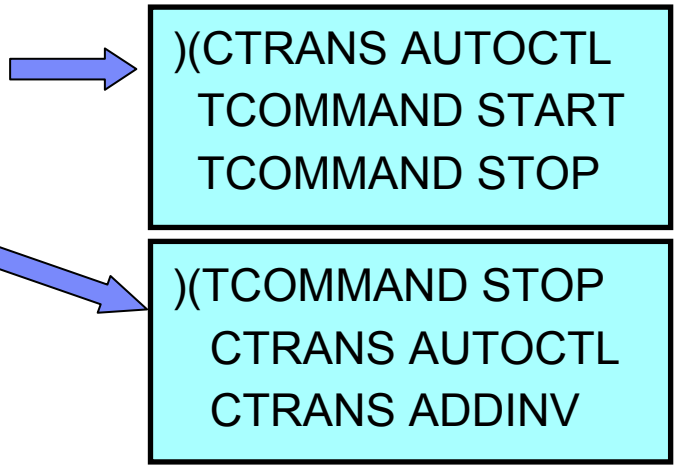
- **Define all AGN resources to RACF in the appropriate classes**
- **Define all region ids as RACF users**
  - BMPs, MPPs, IFPs, etc.
- **Permit region ids to access appropriate resources**
- **Change SECURITY macro to specify RAS**

  and/or
- **Change ISIS= parameter in DFSPBxxx to specify RAS**
- **If needed, add ODBASE=Y to DFSPBxxx**
- **Restart IMS**
- **When safe, remove SMU definitions**

AOI Security

AOI Security in Prior Releases

- **Automated Operator Program commands**
  - **Type 1 AOI - CMD calls**
    - **SMU** transaction command security
    - SECURITY... TRANCMD = NO | YES | FORCE
      /NRE or /ERE COLDSYS ... TRANCMDS | NOTRANCMDS
    - SMU definitions
      - Which commands can be executed by a specific program
      - Which programs can execute a specific command



  - **Type 2 AOI - ICMD calls**
    - **RACF** security &/or DFSCCMD0
    - Checks userid access to CIMS class resources

AOI Security in IMS V9

- **IMS V9 enhancements**

1. **RACF &/or DFSCCMD0 support for**
   - **Type 1 AOI CMD calls**
     and
   - **Type 2 AOI ICMD**

2. **New TRANSACT macro parameter**
   - Defines what is used as the userid
   - Affects both Type1 and Type2 AOI calls
   - But has slightly different meaning for each type

If you make no changes when migrating to IMS V9, AOI security will be as before

Security Support for Type 1 AOI (CMD)

- **New IMS EXEC parameter to choose type of security**
  - **AOI1=** N | C | R | A | S
    - for Type 1 commands only
      - AOIS is parameter for Type 2 commands
    - Provides a choice of SMU or RACF/DFSCCMD0
      - SMU will not be available in future IMS releases

N = No authorization security checking is done (command is permitted)
C = DFSCCMD0 is called for command authorization
R = RACF is called for command authorization
A = Includes options C and R. RACF is called first, then DFSCCMD0
S = SMU security is called for command authorization

    - Defaults to system definition specification (= SMU) on SECURITY macro (as in previous releases)
- **Can be overriden by /NRE or /ERE ... TRANCMDS | NOTRANCMDS**

Use SMU

Use none

Security Support for Type 2 AOI (ICMD)

- **Unchanged from previous IMS releases**

AOIS= N | C | R | A | S

- Same values as with AOI1 …
- … but some values (N and S) have different meanings

N = ICMD Calls are Not allowed
C = DFSCCMD0 is called for command authorization
R = RACF is called for command authorization
A = Includes options C and R. RACF is called first, then DFSCCMD0
S = "Skip" – no authorisation checking

Defaults to N

TRANSACT AOI= Parameter

- **New IMSGEN TRANSACT parameter**
  - **TRANSACT …. AOI= YES | TRAN | CMD | NO**
  - Relates to use of RACF/DFSCCMD0 for both types of AOI command

YES = Requests the USERID of the user who entered the transaction be authorised against the Command (in CIMS class)

TRAN = Requests that the TRANCODE be used as the userid for authorization against the Command (in CIMS class)

➔ transactions have to be defined to RACF as USERIDs

CMD = Requests that the COMMAND CODE (first three characters of the command) be authorised against Trancode (in TIMS class)

➔ the first three characters of IMS commands have to be defined to RACF as USERIDs

NO = AOI Type 1 CMD calls are not allowed

Not relevant for AOI Type 2 ICMD calls - same as YES

Note that Type 2 commands now have additional security options

For Type 1 commands, AOI1=N|S ('None' or 'SMU') will override TRANSACT AOI=YES|NO

RACF Replacement for Type 1 AOI (CMD) SMU Security

OLD

```
)(CTRANS AUTOCTL
  TCOMMAND START
  TCOMMAND STOP

)(TCOMMAND STOP
  CTRANS AUTOTRAN
  CTRANS ADDINV
```

NEW

RACF definitions:

```
ADDGROUP AOCMDS
ADDUSER STO DFLTGRP(AOCMDS)
ADDUSER STA DFLTGRP(AOCMDS)

RDEFINE TIMS AUTOCTL  UACC(NONE)
 PERMIT AUTOCTL CLASS(TIMS) ID(AOCMDS) ACCESS(READ)
```

TRANSACT CODE=AUTOCTL
AOI=CMD

```
ADDUSER AUTOTRAN
ADDUSER ADDINV

RDEFINE CIMS STO  UACC(NONE)
 PERMIT STO CLASS(CIMS) ID(AUTOTRAN, ADDINV) ACCESS(READ)
```

TRANSACT CODE=AUTOTRAN
AOI=TRAN

Specify TRANSACT macro AOI= parameter in IMS definitions

RACF and SMU Coexistence in IMS V9

- **Only relevant for Type 1 AOI (CMD) calls**
  - **AOI1=S**
    - Uses SMU security
    - TRANSACT AOI value ignored
  - **AOI1=R|C|A**
    - Uses RACF and/or DFSCCMD0
    - Settings on TRANSACT are honored
  - **AOI1=N**
    - No authorization checking is done
    - Settings on TRANSACT are ignored
  - **AOI1** not specified
    - Defaults to IMS GEN specification for SMU as in previous releases
- **Final override**
  - /NRE or /ERE ... TRANCMDS | NOTRANCMDS

Migrating Off SMU

Type 2 (ICMD)

- **No action needed, but now have choice of what userid to use**

Type 1 (CMD)

- **Initially, code AOI1=S or use default (SECURITY macro) value to get SMU security**
- **Set up required RACF definitions for type 1 commands**
- **Add AOI=value to TRANSACT macros in IMSGEN**
  - Can use online change
  - Will be ignored for type 1 commands while AOI1= indicates SMU security
- **Change (or add) AOI1=R to DFSPBxxx**
- **Restart IMS**
- **When safe, remove SMU definitions**

Time Control Option (TCO) Security

TCO Security in Prior Releases

- **Time Controlled Operations (TCO)**
  - IMS capability to execute time-initiated commands and transactions
- **Security support**
  - Authorization of loading of TCO script by an LTERM
    - performed only by DFSTCNT0 exit
  - Resource authorization
    - Commands and Transaction security using SMU
    - Transaction security (only) using RACF
      - Command security could be requested but is not performed

TCO Security in IMS V9

- **Loading of TCO scripts**
  - No change - performed only by DFSTCNT0 exit
- **Resource Security**
  - Command and Transaction security with SMU
    - Last release of IMS to provide this
  - Command and Transaction security with RACF

TCO Security with SMU

- **Uses standard SMU transaction and command security, but explicitly for the TCO input LTERM, DFSTCFI**

```
)( TERMINAL    DFSTCFI
        COMMAND    START
        COMMAND    STOP
        TRANSACT    STATTRN

)( COMMAND    START
        TERMINAL    DFSTCFI

)( COMMAND    STOP
        TERMINAL    DFSTCFI
```

- **DFSCCMD0 will also be called if it exists (after SMU check) for command security**

RACF Security for TCO in Prior Releases

- **Requires IMS EXEC parameter, RCF= A | S | R | B**
  - Requests RACF support for transaction and command authorisation
- **Requires a USERID**
  - TCO script specification of `/SIGN ON tcousid tcopw`
    - **`Should also issue /SIGN OFF at end of script`**
  - Else uses control region userid
- **Available for RACF authorization of <u>transactions only</u>**
  - TCO userid is authorised to use transactions in the TIMS class, as usual
- **Command security for TCO userid can be specified …**
  - **… but RACF will not be called**
  - TCO is treated by IMS like a system console or master terminal
    - Eligible to enter any commands
  - DFSCCMD0 will be called if it exists

RACF Support for TCO in IMS V9

- **Requires new execution parameter: TCORACF = Y | N**
  - Specifies whether or not TCO security supports RACF
- **Requires RCF = A | S | R | B** (as previously)
  - RACF is called for TCO security only if TCORACF = Y is also specified
- **Requires a TCO USERID**
  - TCO script specification of `/SIGN ON tcousid tcopw`
    - **`Should also issue /SIGN OFF at end of script`**
  - Else uses control region userid
- **RACF will be called in standard way to authorise transactions and/or commands**
  - Using TCO USERID
- **DFSCCMD0 will be called if it exists (after RACF) for command security**

RACF Support for TCO ...

OLD

```
)( TERMINAL    DFSTCFI
          COMMAND    START
          COMMAND    STOP
          TRANSACT   STATTRN
```

"NEW"

```
ADDUSER  TCOUSID  DFLTGRP(IMS) OWNER(IMS) PASSWORD(SCRIPTS)
PERMIT STA CLASS(CIMS) ID(TCOUSID) ACCESS(READ)
PERMIT STO CLASS(CIMS) ID(TCOUSID) ACCESS(READ)
PERMIT STATTRN CLASS(TIMS) ID(TCOUSID) ACCESS(READ)
```

This example assumes:

- Command and transaction profiles already exist
- The TCO userid (TCOUSID) is connected to a RACF group
- The TCO script issues a /SIGN ON for TCOUSID
- RCF= and TCORACF=Y are specified

The above definitions could have been coded in prior releases. If so, authorization for the transaction was done. Command authorization, however, was never invoked.

In IMS V9 (TCORACF=Y), using the same definitions, RACF will be invoked for command authorization.

Migrating Off SMU

- **Prerequisite is that RACF is used for command / transaction security**
  - RCF= A | S | R | B
- **Define TCO userid and permissions in RACF**
- **Add /SIGN ON (and /SIGN OFF) to all TCO scripts**
- **Add TCORACF=Y to DFSPBxxx**
- **Restart IMS**
- **When safe, remove SMU definitions**

MSC Link Receive Security

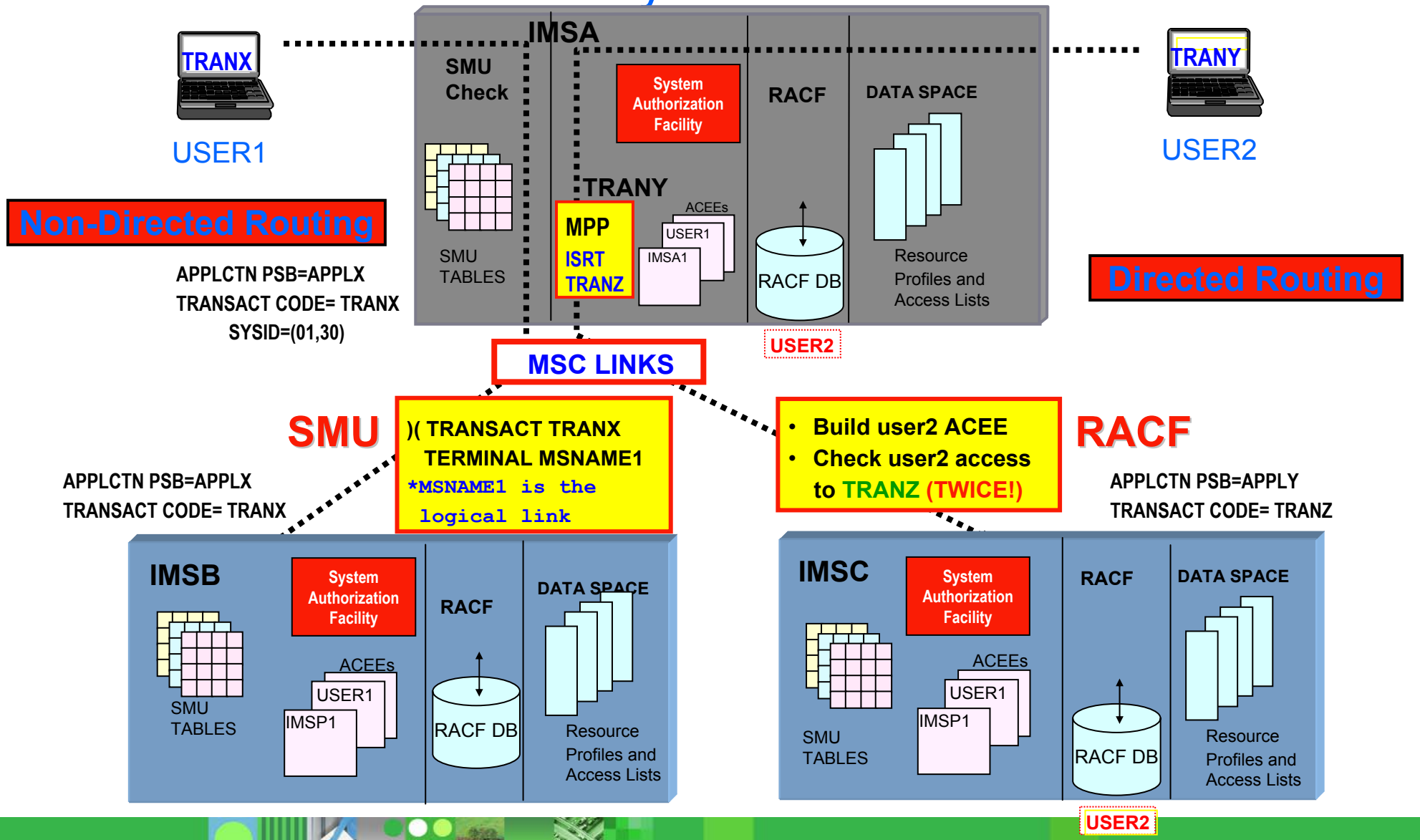
MSC Link Receive Security in Prior Releases

- **Directed Routing***
  - **Uses RACF**, and Transaction Authorization Exit Routine (DFSCTRN0) if defined
  - If DFSMSCE0 exit (link receive entry point) is defined, RACF and DFSCTRN0 are called before and after call of DFSMSCE0
- **Non-Directed routing**
  - **Uses SMU** (after the DFSMSCE0 call)
    - Normal transaction security using MSName as the LTERMname
  - Note: security checking may also have already taken place in the inputting IMS (terminal security or CHNG call security)

Note that Directed and Non-directed routing use different userids for security

* "Directed Routing" is when application explicitly specifies target location
  - Not necessarily defined in IMS GEN

MSC Link Receive Security in Prior Releases …



MSC Link Receive Security in IMS Version 9

- **New DFSDCxxx parameter to specify use of RACF / DFSCTRN0**
  - **MSCSEC=(parm1, parm2)**
    - **parm1 : defines types of MSC link-receive usage that require security**
      - LRDIRECT | LRNONDR | LRALL | LRNONE
    - **parm2 : defines type of security check to be performed**
      - CTL | MSN | USER | EXIT | CTLEXIT | MSNEXIT | USREXIT | NONE

RACF for MSC Link Receive Security in V9

- **MSCSEC=(parm1, ...)**
  - LRDIRECT = Link Receive Directed Routing tran security checking
  - LRNONDR = Link Receive Non-Directed Routing tran security checking
  - LRALL = LRDIRECT and LRNONDR
  - LRNONE = No Link Receive security checking
- **V8 compatibility is provided with LRDIRECT**
  - SMU security will be used for non-directed routing in V9
- **RACF / DFSCTRN0 called once, after DFSMSCE0**
- **The USERID to be used is defined by MSCSEC parm2 or DFSMSCE0 Exit**

RACF for MSC Link Receive Security in V9 ...

- **MSCSEC=(……., parm2)**
  - Specifies type of security checking
  - **MSCSEC**=(LRDIRECT | LRNONDR | LRALL | LRNONE ,

    CTL | MSN | USER | EXIT | CTLEXIT | MSNEXIT | USREXIT | NONE)

CTL	**=**	**Use userid of control region**
MSN	**=**	**Use MSNAME as the userid**
USER	**=**	**Use the terminal user's userid**
EXIT	**=**	**Authorization by user exit alone (DFSCTRN0)**
CTLEXIT	**=**	**Use ctl regn userid for RACF and call DFSCTRN0**
MSNEXIT	**=**	**Use MSNAME as userid for RACF and call DFSCTRN0**
USREXIT	**=**	**Use terminal user's userid for RACF and call DFSCTRN0**
NONE	**=**	**No Security authorization checking**

Note: with RACF, security environment for control region or MSNAME is built once when first used, and retained. But security environment for an end user is built and deleted for each message.

New Role for DSFMSCE0 Link Receive Processing

- **Traditionally, directed and non-directed routing have used different userids for security**
  - To achieve this in future will require the use of DFSMSCE0 exit
- **Additional data is passed to DFSMSCE0**
  - Userid, Group name, and Userid indicator
- **DFSMSCE0 can override MSCSEC PARM2 value**
  - In other words, DFSMSCE0 link receive processing can –
    - Enable or disable security check
    - Enable or disable use of DFSCTRN0
    - Choose what userid to use for RACF security
      - user, control region or MSName

Migrating Off SMU

- **When migrating to IMS V9, add to DFSDCxxx**
  - MSCSEC=(LRDIRECT,USER)
    - or authorise control region for transaction execution, and take default MSCSEC values (LRDIRECT,CTL)
- **Decide what type of userid to use for directed and non-directed routing**
  - Easier when both the same, but can be different
- **Update RACF to include new userids (MSNAMEs and Ctl Rgn) if necessary, and grant their access to transactions**
- **If using two types of userid, code DFSMSCE0 accordingly**
- **Change DFSDCxxx to include**
  - MSCSEC=(LRALL,USER |MSN |CTL)
- **Restart IMS**
- **When safe, remove SMU definitions**

/LOCK, /UNLOCK and /SET Security

/LOCK, /UNLOCK and /SET Security in Prior Releases

- **SMU is used to provide *Password Security***
  - e.g., /LOCK DATABASE payroll (uomecash)
    /SET TRANSACTION paytran (uomecash)
  - Note: these passwords can not be used with ETO terminals (ETO and SMU are incompatible)

Password is associated with specific resource

- **Definitions to achieve SMU /LOCK and /SET password security**
  - IMSGEN SECURITY Macro : PASSWD=YES
    - Can override with /NRE or /ERE COLDSYS PASSWORD
  - SMU Definitions

```
)( DATABASE  PAYROLL
   PASSWORD  UOMECASH
```

or

```
)( PASSWORD UOMECASH
   DATABASE PAYROLL
   PROGRAM PAYPROG
   TRANSACT PAYTRAN
```

Use of /LOCK, /UNLOCK and /SET Security

- **An "end user manager" can LOCK and UNLOCK his users' LTERMs**
  - One or more LTERMs for a physical terminal
  - Only he knows the password to do this (when using SMU)
- **Similarly he can SET the destination transaction code for a terminal**
  - Only he knows the password to do this (when using SMU)
- **Senior operators can LOCK and UNLOCK DBs, programs and transactions**
  - Only they know the passwords to do this (when using SMU)
- **In IMS V9 with RACF, these "special people" are explicitly authorised to LOCK, UNLOCK and SET specific resources**

RACF /LOCK, /UNLOCK and /SET Security in IMS V9

- **New DFSDCxxx parameter : LOCKSEC = Y | N**
  - **N = No authorization checking**
    - standard command security will still apply
  - **Y = Calls RACF** (and DFSCTRN0 if TRAN)
    - RACF classes: LIMS, PIMS, IIMS, TIMS
      - for LTERM, DB, PSB, TRAN respectively
    - If resource is not defined to RACF, access will be granted

Does not apply to /LOCK or /UNLOCK of NODE or PTERM

- **RACF security is based on user's userid**
  - Userid must be authorised to issue /LOCK, /UNLOCK, /SET commands AND must be authorised for use of specific resource
- **This is not an alternative to SMU password security**
  - SMU checking will be done first, if defined, and then the RACF checks will take place

Migrating Off SMU

- **Define to RACF all resources that need to be LOCKed or SET**
  - LTERMs, DBs, Programs (PSBs), and Transactions
- **Grant authority for using these resources to the appropriate userids**
- **Add LOCKSEC=Y to DFSDCxxx**
- **Restart IMS**
- **When safe, remove SMU definitions**
- **Inform users that passwords are no longer needed**

Sign On Verification Security

Signon Verification Security

- **SMU method for static terminal Signon Verification**
  - Defines which static (non-ETO) terminals must /SIGN ON

```
)( SIGN
        STERM TERM1
        STERM TERM2      }  or      STERM ALL
        STERM TERM3
        ...
```

  - Requires
    - SECURITY SECLVL=SIGNON or FORCSIGN
  - … and typically requests RACF verification of userid/password with
    - SECURITY TYPE=RACFTERM

Signon Verification Security in IMS Version 9

- **Does not require RACF** (or SMU)
- **New startup parameter in DFSDCxxx**
  - **SIGNON = ALL | SPECIFIC**
    - ALL : all static terminals (except 3284/3286, SLU1 printers, and MTOs)
    - SPECIFIC : based on OPTIONS of TYPE/TERMINAL macro
- **Addition to the OPTIONS parameter on the TYPE and/or TERMINAL macros**
  - **OPTIONS = (...,SIGNON | NOSIGNON)**
    - Specification on TERMINAL macro overrides TYPE
- **If a TERMINAL has both a SMU specification (i.e. sign-on required) and a conflicting OPTIONS=NOSIGNON, then SMU takes precedence**

Migrating Off SMU

For "ALL"

- Add SIGNON=ALL to DFSDCxxx
- Restart IMS

For "SPECIFIC"

- Add OPTIONS=(…SIGNON…) for all TERMINALs which currently have an explicit SMU signon requirement
- Add SIGNON=SPECIFIC to DFSDCxxx
- Restart IMS

- When safe, remove SMU definitions

Other Considerations

LTERM Security

SMU

1. Controls static LTERM availability through password security:
   - /LOCK and /UNLOCK LTERM (pswd)
2. Protects which static LTERMs can be used in NMD BMP and JBP specification of OUT=
   - AGN definitions
3. Provides additional protection for signed on static terminals:
   - requires the user to enter the SMU-defined password that is associated with the transaction or command

SAF / RACF

1. Checks the userid authorization to the resource using:
   - the new resource class LIMS when LOCKSEC=Y
2. Uses RAS security based on SECURITY macro TYPE= RASRACF|RASEXIT|RAS|NORAS or override value of ISIS=N|R|C|A
   - Checks userid associated with NMD BMP or JBP for authorization to the LTERM using the new LIMS class
3. Uses the REVERIFY facilities in IMS and RACF by specifying RVFY=Y in IMS and 'REVERIFY' in the APPLDATA section of the RACF profile for the commands and transactions to be protected
   - Requires a signed on user to reenter his/her signon password with the transaction or command input

LTERM Security …

SMU

4. Restricts entry of certain commands to specific static LTERMs
   - SMU definitions
     e.g.,)(COMMAND DIS
     TERMINAL LTERMA

)(TERMINAL LTERM5
     COMMAND DIS
     TRANSACT TRAN

5. Restricts entry of certain transactions to specific static LTERMs
   - SMU definitions
     e.g.,)(TRANSACT PAYROLL
     TERMINAL LTERMB

SAF / RACF

4. Restricts entry based on a combination of RACF and DFSCCMD0. The first check is the RACF call to validate if the userid can enter the command.
   - If DFSCCMD0 exists, it is always invoked and can make the second call. Possible alternatives:
     - Create FACILITY class RACF profiles of command.lterm, e.g., DIS.LTERMA. These would equate to the combinations defined in SMU. In DFSCCMD0, call RACF to authorize userid/groupid to the resource class using the applicable resource combinations.
     - Or, protect all the static LTERMs with the new LIMS resource class. Define the commands (there are about 50) as userids. In the exit, invoke RACF to VERIFY the IMS command (build the ACEE) as a userid, and authorize it against the LTERM name.

5. Similar techniques as described above for restricting commands. DFSCTRN0 is used instead of DFSCCMD0

Migration Considerations

- AOI considerations
  - CMD has new status code and new return/reason (AIB) codes
  - ICMD has new return/reason codes
- Log record (type X ‘10’) has new error codes
- New and changed Exits
  - DFSRAS00, DFSCCMD0, DFSISIS0, DFSMSCE0
- New RACF security classes
  - IIMS, JIMS, LIMS, MIMS
    - Predefined in z/OS 1.6
- Changing RCF from “N” to something else requires a cold start

Summary

- **Prior to IMS V9, there are six security functions that are only possible with SMU**
  - They can still be implemented with SMU in IMS V9
  - But this will not be so in the follow-on release of IMS
    - **IMS V9 is last release to support SMU**
- **IMS V9 introduces new facilities that enable these six security functions to be implemented with RACF (or equivalent product)**
  - Also adds some new security functions
- **Recommend: all users of SMU should install IMS Version 9 and then migrate all SMU functions to RACF while on this release**