Information Management

IBM

IMS Rock-Solid Security in the Post-SMU Era

August 2009

Data Management

Alan Cooper
IMS Consultant
alan_cooper@uk.ibm.com

Disclaimer

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

The Need for Rock Solid Security in IMS

- **The days of SMU security with a well known set of predefined LTERMs are long-since gone**
- **Even the days of just a well known group of RACF userids are gone**
- **IMS systems are being *opened up* in this era of TCP/IP, SOA, Web 2.0, B2B, etc.**
  - Many more known end-users
  - Access by unknown end-users
  - Access to IMS TM via multiple channels
    - LU2, APPC, OTMA, etc
- **Increased threat from hacking, internal misuse, etc.**
- **Growing emphasis on security auditing**

IMS security needs to be

ROCK SOLID

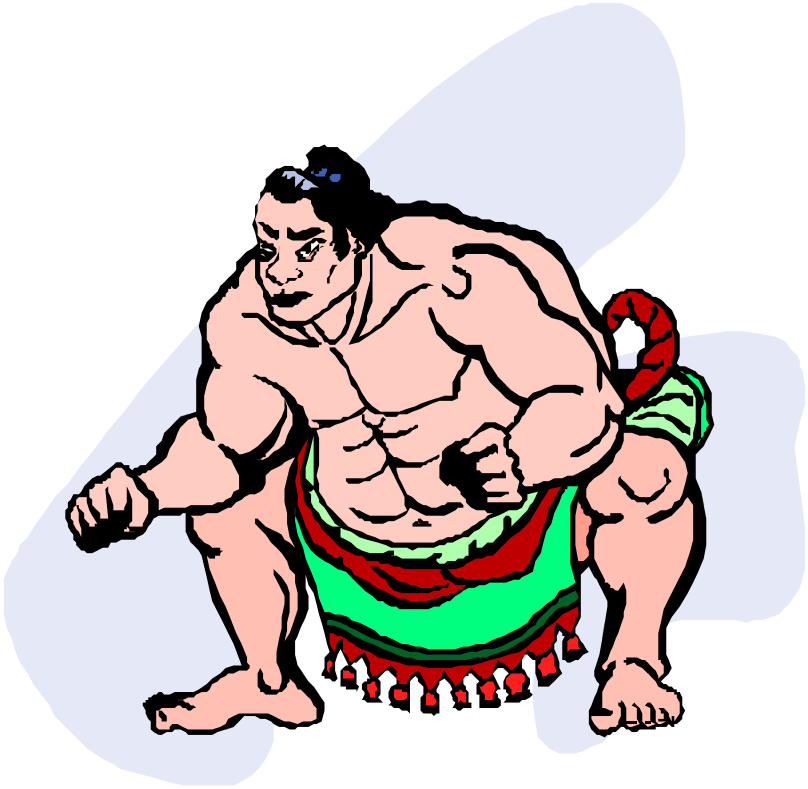
Agenda

- What RACF can provide for IMS
- IMS Dataset Security
- IMS Transaction Manager Security
- DBRC Security
- End User Issues
- Security Auditing

What RACF Can Provide for IMS

Resources Protected by RACF

- **RACF can be used to protect against unauthorised access to a variety of resources including –**
  - IMS system
  - IMSPlex
  - IMS XCF Groups
  - IMS Structures in Coupling Facility
  - IMS System datasets
  - IMS Databases
  - IMS Transactions
  - IMS Commands (Type 1 and Type 2)
  - IMS Programs/PSBs
  - RECON data



RACF Userids

- **RACF security is about controlling access to resources by Userids**
- **With IMS, there are various potential types of userid**
  - Real end-user userids
    - Entered via /SIGN ON at SNA terminal
    - Passed in OTMA Prefix by OTMA Client
  - Default userids representing end-users
    - e.g. set by IMS TM Resource Adapter or IMS Connect in OTMA Prefix
  - Region IDs
    - For IMS system address spaces and dependent regions
  - Convenience userids
    - Userids with same name as a Transaction, IMS command verb, NMD-BMP PSB, MSC MSNAME, or LTERM
- **Region IDs – and particularly the Control Region's ID – are sometimes used because no other userid is available**
  - But is this appropriate when thinking of "Rock Solid" security???

IMS Security Exits used with RACF

- **Many (most) aspects of IMS security can be implemented with either or both of RACF and IMS User Exits**
  - e.g Sign On User Verification – DFSCSGN0 Signon/off security Exit
    Transaction Authorisation – DFSCTRN0 Transaction Authorisation Exit
    Type 2 Command Authorisation – CSL OM Security User Exit
    DBRC Command Authorisation – DSPDCAX0 DBRC Command Authorization Exit
    etc. etc. etc.

- **Where standard security can be fully implemented with RACF, no mention of the Exit will be made in this presentation**

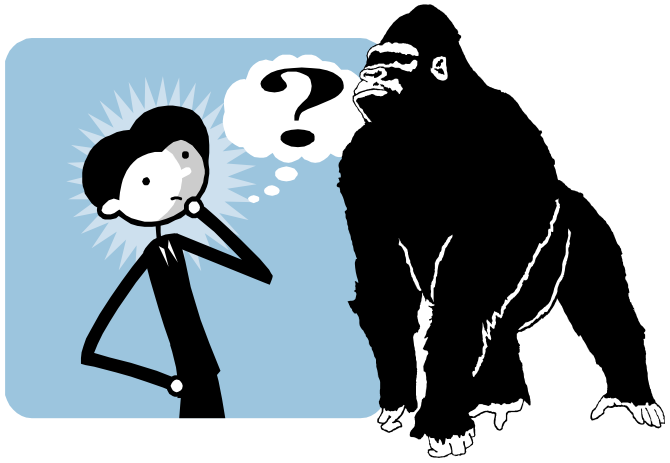
- **But the Exit will be mentioned in those special cases where it is the only way to provide a potentially desirable option**

How IMS Uses RACF

- **At IMS Start-up, IMS issues –**
  - **RACROUTE REQUEST=LIST,GLOBAL=YES**
    - Builds resource profiles for the IMS resource classes (defaults are TIMS, GIMS, CIMS, DIMS, etc) in a dataspace
  - **RACROUTE REQUEST=VERIFY,ENVIR=CREATE,ACEE=addr…..**
    - Builds ACEEs for IMS, DLISAS, DBRC address space userids

- **When a user SIGNs ON**
  - **RACROUTE REQUEST=VERIFY,ENVIR=CREATE,ACEE=addr…..**
    - IMS passes USERID, GROUP, PASSWORD, TERMID, APPL
    - To build ACEE for the userid

- **When a resource access is requested (e.g. Before queueing a transaction)**
  - **RACROUTE REQUEST=FASTAUTH …**
    - Passing User's ACEE, name of class, and name of resource

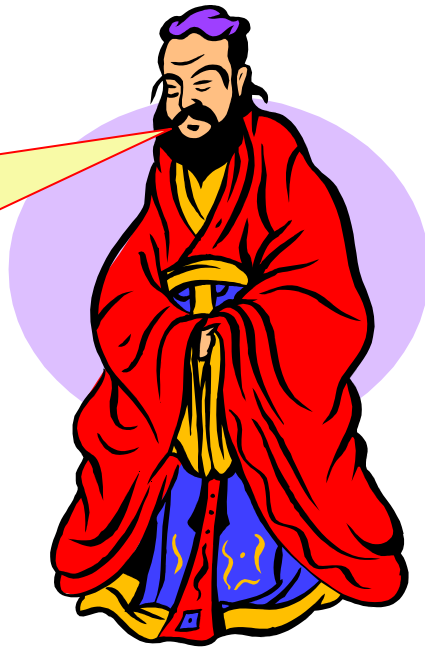


IMS Dataset Security

IMS Dataset Security

- **In 1976, when RACF first became available, its sole function was to provide Dataset Access security**
- **IMS has two types of dataset**
  - System datasets
  - Database datasets
- **Dataset Access Security for both types of IMS dataset is fundamental to all other forms of IMS security**

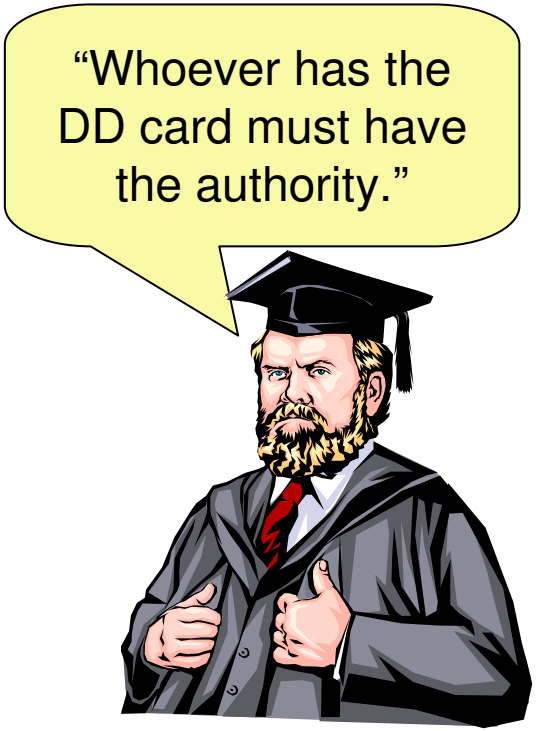
> *"If access to the IMS database and library resources is not controlled, further access control within IMS is of little value because the controls within IMS depend on these resources."*



- **RDEFINE all IMS system datasets and DB datasets**
  - With UACC(NONE)
- **Ensure that catalogs are also RACF-protected**

IMS Dataset Security Userids

- **Each IMS system address space needs to have an associated userid**
- **To run as a started procedure, the RACF recommendation is to add the procedure name as an entry in the STARTED class**
  - Identifies the userid to be associated with the procedure
  - Alternatively, add the procedure's name to the RACF started procedures table (ICHRIN03)
- **Address Space Userids should have the PROTECTED attribute**
  - PROTECTED = NOPASSWORD + NOOIDCARD + NOPHRASE
    - NOOIDCARD is default on ADDUSER (to register a new userid)
    - NOPHRASE is implicit default if use ADDUER without PHRASE
  - **Ensures that no one can logon using the address space userid**
- **Control Region and DLISAS can share a userid**
  - But do not use the same userid for system address spaces and dependent regions
- **PERMIT each dataset to be used by appropriate region-ids, batch/utility users, and systems personnel**
  - IMS itself requires CONTROL access to DBDSs



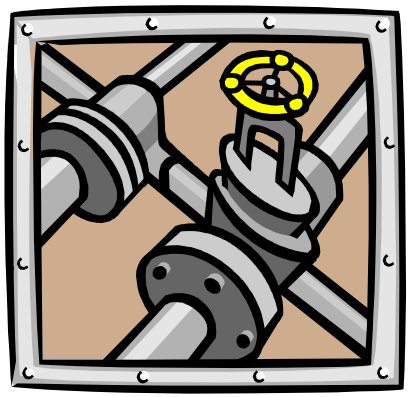
IMS Transaction Manager Security

IMS Parameters

- **Security requirements are specified in the IMS system definition and in execution parameters**
- **In the system definition, use just the SECURITY macro for security specification**

```
SECURITY RCLASS=……,SECCNT=……,SECLVL=……,TYPE=……
```

  - Remove security specifications from COMM and IMSGEN macros
    - Your successor might not be used to the flexibility of the traditional IMS world!
- **RCLASS can be on SECURITY macro or in the DFSDCxxx member**
  - DFSDCxxx takes precedence
  - If you have only one IMS system (or IMSplex) with security enabled, then the default IMS RACF security classes (pre-defined in module ICHRRCDX) are fine
    - TIMS, GIMS, CIMS, DIMS, etc.
  - Otherwise, define a parallel set of classes in RACF for each IMS system (or IMSplex) and use the RCLASS parameter to identify them to IMS
    - e.g. RCLASS=IMP4 → TIMP4, GIMP4, CIMP4, DIMP4, etc
    - Note: To set up new classes, RACF recommends using Dynamic Class Descriptor Table (CDT) rather the static module, ICHRRCDE
- **SECCNT is unique to the SECURITY macro**
  - No JCL override



IMS Parameters …

- **SECLVL and TYPE parameters can all be overridden by Execution Parameters in DFSPBxxx**
  - **Recommend**: omit them or set them to match the execution parameters
- **SECLVL – is used to indicate that some form of security (RACF &/or Exits) is to be used at User SIGNON and for Transaction Authorisation**
  - Also indicates if this specification can be disabled by operator at IMS restart
  - Best RACF security will be with

    SECLVL=(FORCTRAN,FORCSIGN) ←→ TRN=F,SGN=F
  - Note: this enables signon verification to take place when a user signs on, but does not itself force users to sign-on!
- **TYPE – provides more specific list of what security is required**
  - But **DFSPBxxx parameters** provide more options, and are thus **recommended**
    - **RCF=**A → use RACF for signon verification, and transaction and command authorisations for static and ETO terminals
    - **ISIS=**R → use Resource Access Security

Other Security Execution Parameters

DFSPBxxx

- AOI1, AOIS = auto-ops command security*
- CMDMCS = MCS/E-MCS command option*
- ODBASE, APPCSE, OTMASE = security options for ODBA, APPC and OTMA
- TCORACF = Time Control Option (TCO) use of RACF Command Authorisation*
- RVFY = RACF reverify option*
- RCFTCB = Number of RACF TCBs (1 – 20)
- ALOT = default automatic logoff time for ETO terminals
- ASOT = default automatic signoff time for ETO terminals*

DFSDCxxx

- BMPUSID= security userid for NMD-BMP*
- MSCSEC = MSC link receive security options*
- LOCKSEC= security options for /LOCK, /UNLOCK and /SET commands
- SIGNON= static terminals “sign-on required” specification*
- SAPPLID= APPL name to be used with pass tickets

* Items in black are discussed on later slides

Forced User Sign-On

- SECURITY macro, and SGN= and RCF= execution parameters can be set to ensure that RACF is called when a user enters a /SIGN ON command
  - But does not force the use of /SIGN ON
- Sign On is required at ETO terminals
- For Static terminals, *none*, *some*, or *all* terminals can be defined to require signon

- DFSDCxxx → SIGNON=ALL

or

- DFSDCxxx → SIGNON=SPECIFIC

together with

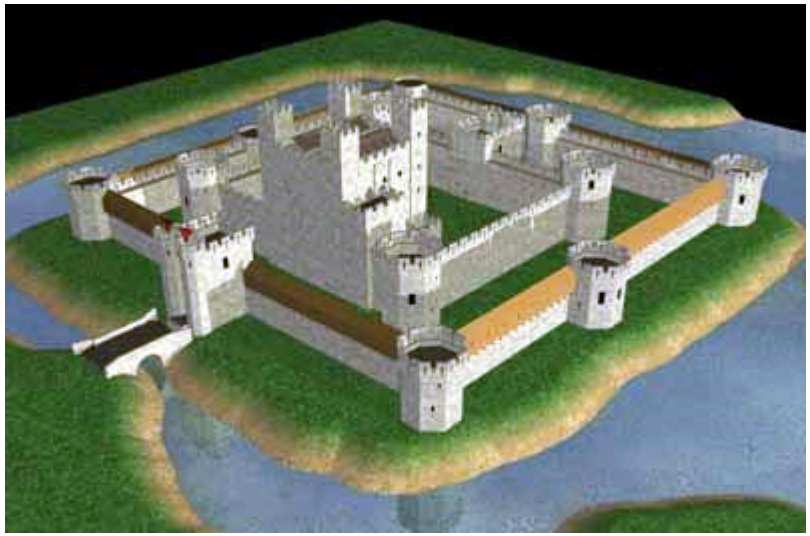
IMS System Definition → TERMINAL OPTIONS=(…,SIGNON,…)

IMS Region IDs

- **Earlier, it was mentioned that the IMS System Address Spaces should have userids assigned**
  - Used with dataset access control
  - And optionally for some other system functions
- **Dependent Regions should also have userids assigned**
  - Dependent Region Ids are used for connection security and Resource Access Security (RAS)
  - Should be different ids from system address space ids
- **Dependent Region Userids should, like the system address spaces, have the PROTECTED attribute**

- **Both System Address Space and Dependent Region userids should also have the RESTRICTED attribute**
  - They will only be allowed to access resources for which they are explicitly permitted
    - PERMIT …. ID(*) → will deny access to RESTRICTED userids
    - UACC(READ) → will deny access to RESTRICTED userids

IMS Connection Security



- **"Stopping the enemy at the outer defences"**
- **There are two types of IMS Connection Security**
  1) Controlling which users can **SIGNON** to a specific IMS
     - And optionally from which VTAM terminals
  2) If RAS is enabled, controlling which Dependent Regions can connect to Control Region
- **Each protected IMS system must be RDEFINEd in the RACF APPL class**
  - RDEFINE APPL (IMP4, IMP6) UACC(NONE)
- **User Connection Security**
  - PERMIT IMP4 CLASS(APPL) ID(USRGRP1,COOP*) ACCESS(READ)
  - PERMIT IMP6 CLASS(APPL) ID(USRGRP8) ACCESS(READ)
    WHEN(TERMINAL(NODE01,NODE9*))
- **Dependent Region Connection Security**
  - PERMIT IMP4 CLASS(APPL) ID(MPRGRP1,MYBMP*) ACCESS(READ)
  - Requires Resource Access Security (RAS) be activated

SNA Terminal Security

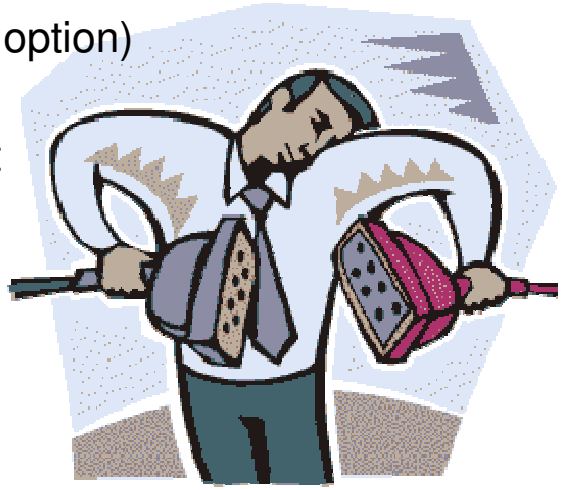
- **Terminal security is a general RACF facility for SNA terminals that can be exploited with IMS**
  - Another check that takes place at end-user SIGNON time
    - "*Is the userid authorised to use the terminal?*"
  - Terminals are RDEFINEd in the TERMINAL class (Grouped in GTERMINL class)
  - In addition, RACF can limit terminal access to certain times and/or days of the week
    - RDEF TERMINAL(NODE123) WHEN(DAYS(WEEKDAYS) TIME(0800:1700))

- **The Terminal Access check and the User Connection check (previous slide) both take place at user SIGN ON**
  - SIGNON Verification must be enabled (e.g. SECLVL SIGNON, or SGN=F, etc.)

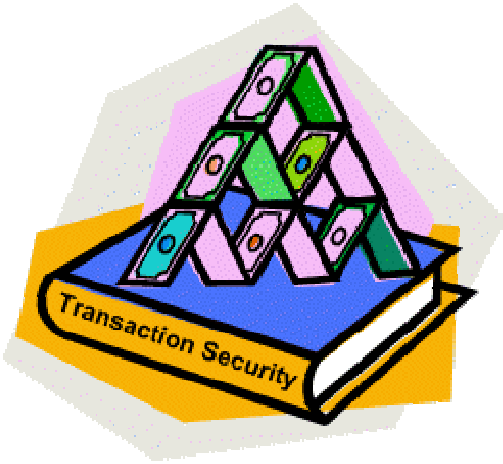
    and
  - User must be forced to Sign On

Security with IMS Connect

- **Security for access via IMS Connect is equally tight**
- **IMS Connect has a userid which is used for Client Bid (connection to IMS) security**
  - "Is it the right userid for this IMS Connect and is it allowed to connect to this IMS?"
  - Implemented by defining OTMA XCF group and member names in FACILITY class
- **In IMS 10, IMS Connect can specify an ACEE Ageing Value for OTMA ACEE caching**
  - How long OTMA can keep an ACEE for a userid of an IMS Connect user
- **IMS Connect's client can perform user validation and send input containing userid and a pass ticket …**
- **… Or can send a userid and password**
  - IMS Connect can validate userid with RACF (IMS Connect configuration option)
  - If you use an IMS Connect Security Exit (link edited with User Message Exit), you can perform any RACF user validation and other checking that you deem necessary
- **When message reaches IMS**
  - OTMA will verify userid by building the ACEE (if not already done)
  - Then standard transaction and command security will apply



Transaction Security



- **The foundation of IMS Transaction Manager security**
  - "*Is the userid authorised to use the transaction?*"
- **RDEFINE transaction codes in the TIMS class (or your equivalent), or more conveniently, group those with similar security requirements in the GIMS class, and PERMIT appropriate groups of users to access the transaction groups**
- **As with most RACF classes, RDEFINE a "catch all" generic transaction with name "**" and UACC(NONE)**
  - Ensures all transactions – existing and future – must have their security explicitly defined before they can be used
- **As a "belt and braces" approach, you can set up (or RALTER) a class to have DEFAULTRC(8)**
  - If resource not defined, then RACF will set return code for "deny authorisation"
- **If a transaction can be used by "anyone", note the difference between –**
  - RDEFINE transaction with UACC(READ)
    - Access is truly unrestricted
  - PERMIT …. ID(*) ACCESS(READ)
    - Access is only allowed for defined userids (except RESTRICTED userids)

Transaction Security …

- **Some customers have a need for even tighter transaction security -**
  - **Some transactions are only to be entered at certain terminals**
  - Perhaps in a building with more restricted access
- **The standard technique is to use a combination of RACF transaction security and the IMS Transaction Authorisation Exit (DFSCTRN0)**
  - Exit has a table of terminals against transactions
- **Some customers are reluctant to use IMS Exits due to declining Assembler skills**
- **One alternative approach is to allocate an additional "special userid" to each user who is authorised to enter these sensitive transactions at the restricted terminals**
  - Use RACF terminal security to ensure that only the "special userids" can sign on at the restricted terminals, and that they can not sign on with the special ids at other terminals
  - Sensitive transactions are only authorised for use by the special userids

Transaction Security When There is No Userid

- **Messages coming in via OTMA usually have an associated userid – although this might be a default id set by IMS TM Resource Adapter or IMS Connect**
- **ETO terminals and Forced Sign-On Static terminals will be signed-on and have a userid**
  - Note: ETO and static terminals can be AUTO-SIGNed-ON at LOGON time
    - Requires use of Logon Exit (DFSLGNX0)

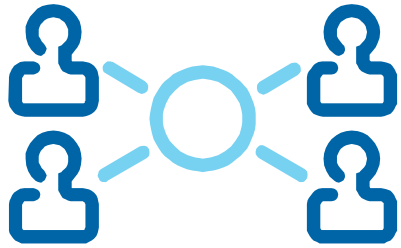
- **But some static terminals can be used without sign-on**
  - **There will be no connection or terminal security**
  - **When IMS calls RACF for transaction authorisation, there will be no user ACEE. So the home address space userid will be used, namely the Control Region Id**
- **Either PERMIT Control Region Id to use the unrestricted transactions**
- **Or RDEFINE unrestricted transactions with UACC(READ)**
- **A better, more explicitly controlled, solution would be if Static LTERMs could be defined to automatically sign-on with Userid=LTERMname**
  - The requirement is well understood : see APAR PK85571

CHNG and AUTH Call Transaction Security

- **When an IMS online application issues a CHNG call for a transaction, or issues an AUTH call with the TRAN sub-function, RACF is called to authorise the use of the transaction**
  - For a message driven application, end-user's userid is used
  - For a NMD-BMP, userid is determined by DFSDCxxx parameter, "BMPUSID"
    - Either Job card's USER=userid, or PSBname

- **In some situations, information about the user (the ACEE control block) is not available in the dependent region**
  - With MSC, when program is running on a 'remote' IMS
  - With Shared queues, when the processing system is different from the inputting system
  - If user Signed Off before transaction processed
- **The ACEE needs to be built in the dependent region**
  - It will happen automatically, but you can potentially enhance performance by use of DFSBSEX0 Exit (for non-OTMA, non-APPC), or the APPCSE or OTMASE execution parameters
    - If CHNG/AUTH call is not used in every occurrence of a transaction, build ACEE dynamically
    - If one or more CHNG/AUTH calls are typically used by a transaction, building ACEE "up front" will give best performance

MSC Transaction Security



- **An IMS Transaction message will have transaction authorisation checking performed when it arrives in its first (or only) IMS system, and before the message is queued to its next destination**
  - Local transaction or MSC link
- **When it arrives at its final destination via MSC, it can again undergo a RACF Transaction Authorisation**
  - You can disable this, or specify the userid to be used, on the DFSDCxxx parameter, MSCSEC=
  - USERID can be -
    - Receiving Control Region (the default!)
    - MSC link MSNAME
    - The end-user's userid

    } Best for efficiency as ACEE is built once and kept for ever
  - Or you can dynamically make the choice in the link-receive entry point of the DFSMSCE0 exit
- **If Trancode is unchanged, or set by a front-end application CHNG call, then it is appropriate to perform back-end security with the MSNAME (and get the enhanced performance)**
- **If Trancode is changed by DFSMSCE0 (link receive), then the end-user's userid might be the more appropriate one to use**

Command Security (via terminals and consoles)

- **IMS Type 1 Commands – first three letters of command verb – are defined in the CIMS class (or your equivalent), or more likely, grouped in the DIMS class**
  - RDEFINE DIMS ENDUSER OWNER(IMS) UACC(READ)
  - RALTER DIMS ENDUSER ADDMEM(BRO CAN DIS END EXC EXI FOR + HOL LOG LOO RCL RCO RDI REL RES RML SET SIG TES)
- **Recommend: Keep it simple! – be consistent in use of RDEFINE UACC and PERMIT ACCESS, especially if a command is in multiple command groups**
- **Security check is simply, "*is user allowed to use the command verb?*"**
- **If you want greater granularity …**

  e.g. /STOP DB v. /STO NODE

  … you need to use the IMS Command Authorisation Exit (DFSCCMD0)
- **There is no RACF command security for commands entered at the MVS System Console or the IMS Master Terminal**
  - If you want to restrict commands that can be entered at the Master Terminal, you need to use the IMS Command Authorisation Exit (DFSCCMD0)
- **MCS and E-MCS console users have a userid. Command security (none, exit, RACF, both) is determined by DFSPBxxx parameter, CMDMCS=**

Command Security via Operations Manager

- **In an IMSplex, commands can be entered via a SPOC to an Operations Manager**
  - Type-1 → /DIS, /DBR, /STO, /CHE, etc
  - Type 2 → QUERY, UPDATE, DELETE, INIT, TERM, QUEUE, CREATE, IMPORT, EXPORT
- **All Common Service Layer address spaces undergo a security check when they register with SCI to try to join the IMSplex**
  - SPOCs, Operations Managers, Resource Managers, IMS Control Regions
  - Resource representing the IMSplex is defined in RACF FACILITY class
- **Type-2 command security can only be performed in OM**
- **Type-1 Command security can be performed in OM, IMS, or both**
  - CSLOIxxx CMDSEC= → OM use of RACF, Exit, Neither or Both (type-1 & type-2)
  - DFSCGxxx/DFSDFxxx CMDSEC= → Type-1 command security in IMS for commands from OM (RACF, Exit, Neither, Both)
- **Recommend: Do all security in OM**
  - More efficient and more granular

Command Security via Operations Manager …

- **RACF OM Command Security**
  - IMS Commands (Type-1 and Type-2) RDEFINED in OPERCMDS class
    - Supports **command_verb . primary_keyword** in combination

  e.g. RDEFINE OPERCMDS **IMS.CSLPLEXA.INIT.OLC** UACC(NONE)
  PERMIT **IMS.CSLPLEXA.INIT.OLC** CLASS(OPERCMDS) ID(ALAN) ACCESS(UPDATE)

  RDEFINE OPERCMDS **IMS.*.STA.DC** UACC(NONE)
  PERMIT **IMS.*.STA.DC** CLASS(OPERCMDS) ID(FRED) ACCESS(UPDATE)

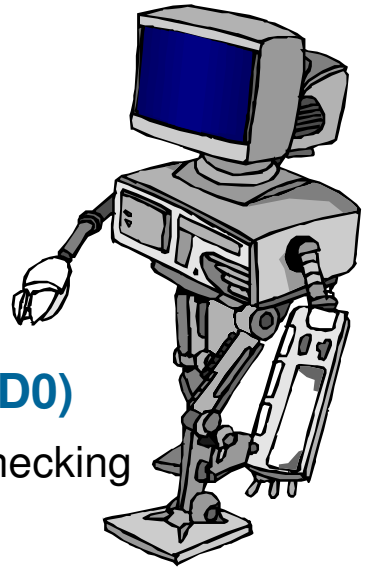
- **Security based on a secondary keyword must be done with the OM Command Security Exit (defined in BPE exits list). Especially relevant for some Type-2 commands - for example -**
  - … NAME(*)
  - QUEUE TRAN …. OPTION(**DEQALL**)

- **Note: QUEUE TRAN … OPTION(ENQ) … will drive normal transaction security checking after the command security has succeeded**

Time Control Operations Security

- **TCO scripts can issue IMS Commands and Transactions, based on various types of time criteria**
  - IMS Control Region JCL “DFSTCF DD statement” identifies the script library
  - This library should have very good RACF protection!
- **Script “DFSTCF” is loaded automatically at IMS startup**
- **To change the script, an LTERM or application sends a formatted “LOAD” message to LTERM, “DFSCTF”**
  - **TCO CNT Edit Exit (DFSTCNT0) is used to authorise the change of script**
  - No option for RACF security at this time
- **Script should contain a /SIGN ON command to set the Userid**
  - Otherwise Control Region Userid will be used for RACF checking
- **RACF transaction authorisation will take place as normal**
- **RACF command authorisation will take place if TCORACF=Y in DFSPBxxx**
  - With TCORACF=N (default), commands will execute without RACF Command Security
- **Do not include a /SIGN OFF in the script**

Automated Operator Programs



- **AO programs execute IMS Commands with either CMD calls (type- 1 AO) or ICMD calls (type-2 AO)**
  - MPP and MD-BMP can use CMD
  - MPP, MD-BMP, and NMD-BMP can use ICMD
- **Command security is provided by RACF in both cases (&/or DFSCCMD0)**
  - DFSPBxxx parameters AOI1= (for CMD) and AOIS= (for ICMD) define security checking
- **For NMD-BMP, userid is from JOB USER=userid**
- **For transactions (MPP or MD-BMP), there is a choice, as specified on TRANSACT macro –**
  - AOI=YES → authorise User USERID (or LTERM if signed off) against command in CIMS
  - AOI=TRAN → authorise trancode as a userid against command in CIMS
  - AOI=CMD → authorise command verb (1st 3 chars) as a userid against trancode in TIMS
    - **CMD and TRAN are probably the most appropriate, as it might not be desirable for AO transaction end-users to be directly authorised to use IMS commands**
- **The relevant trancodes &/or command verbs will need to be defined as RACF userids**
  - Assign PROTECTED and RESTRICTED attributes to these “convenience userids”

Resource Access Security (RAS)

- **Resource Access Security may alternatively be called *Dependent Region Security***
- **Requested on SECURITY macro (TYPE=) or DFSPBxxx ISIS= parameter**
- **Security requirements of BMPs are particularly addressed by RAS**
  - "*is the BMP's userid authorised to use this IMS system?*"
  - *"is the BMP's userid authorised to use the BMP's PSB?"*
  - "*is the BMP's userid authorised to process the transaction specified with IN=trancode*"
  - "*is the BMP's userid authorised to create the transaction specified with OUT=trancode*"
- **More generally, RAS checking takes place at every program schedule (e.g. at BMP statup, MPP program schedule, etc.)**
  - MPP → checks dependent region userid authorised to use trancode (in TIMS)
  - IFP → checks region id authorised to use PSB (in IIMS)
  - BMP → checks USER=userid authorised to use PSB (in IIMS) , IN= trancode (in TIMS), OUT= trancode (in TIMS) or OUT= LTERM (in LIMS)

- **Dependent Region Connection Security (**e.g. "*is the BMP's userid authorised to use this IMS system?*"**) requires (a) RAS to be activated and (b) IMS systems to be defined in RACF APPL class**

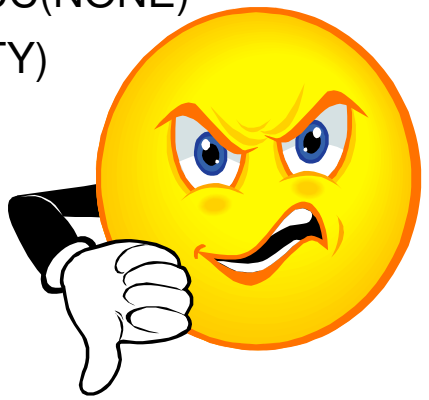
DBRC Security

DBRC Security

- **The RECONs hold data that is critical for DB integrity after failure situations**
  - And hence require a high level of security
  - Especially since they might be accessed by many end users as well as IMS itself
- **RECON Access Security**
  - Prior to IMS 10, there is very limited security available for controlling RECON access
    - People allowed to DELETE/DEFINE the RECON require ALTER access level
    - All other users (including IMS) require CONTROL access
      - **They have full update access to VSAM Records or Control Intervals!**
  - IMS 10 addresses this exposure
    - People allowed to DELETE/DEFINE the RECON require ALTER access level
      - DBRC address space should have ALTER access if Parallel RECON Access is enabled
    - Those allowed to update RECON (e.g. Users of utilities or DB tools, and IMS itself) require UPDATE access
    - People who are only allowed to read the RECON (typically using the LIST command) require READ access
      - Program must issue “OPEN - For Input”
      - So JCL for DBRC Utility (DSPURX00) must include PARM(READONLY)

DBRC Security …

- **DBRC Command Security**
  - Once RACF has authorised access to the RECON data set (at OPEN time), it can then be used to authorise use of DBRC commands by -
    - DSPURX00 utility
    - HALDB Partition Definition Utility
    - /RMxxx commands → after IMS Command processing has authorised the /RMxxx command
    - DBRC API in IMS 10 (IMS 9 only supported QUERY API)
  - DBRC Command Security is enabled by setting flags in RECON header
    - CHANGE.RECON CMDAUTH(SAF|EXIT|BOTH|NONE,safhlq)
  - DBRC Commands are defined in RACF FACILITY class
    - RACF Resource is **safhlq.Command_verb.Resource_type.Resource_name**
    - e.g RDEFINE FACILITY IMP4.GENJCL.RECOV.LEDGERDB UACC(NONE)
      PERMIT IMP4.GENJCL.RECOV.LEDGERDB CLASS(FACILITY)
      ID(COOPER) ACCESS(READ)
    - The valid combinations of verbs and resource type are documented in
      - *IMS 9 DBRC Guide and Reference*
      - *IMS 10/11 System Administration Guide*



End User Issues

IMS End User Aspects of Security

- **Passwords/PassTickets**
  - In client/server situations (where IMS is the server), RACF supports PassTickets
    - A more secure technique than sending passwords over the network
    - IMS and IMS Connect support passtickets or passwords

- **Mixed Case passwords**
  - Mixed-case passwords are more secure and harder to guess than uppercase passwords
  - RACF can be enabled to support them
  - IMS 10 and IMS Connect 10 can be set to support them
    - DFSPBxxx PSWDC= and HWSCFGxx HWS PSWDMC=
  - Note: Turning on mixed case has no immediate impact on IMS end users. Only after a user next changes his password will he then be required to enter the password with the correct case

IMS End User Aspects of Security …

- **ETO Autosignoff**
  - In high-security implementations, ETO end-user terminals should have a sensible Auto Sign Off value (ASOT) set
    - To minimise risk of a different user using the signed-on terminal
    - ASOT is a DFSPBxxx parameter, and can be overridden at SIGN ON using value on ETO User Descriptor or as set by ETO Sign On Exit

- **Password Reverification**
  - Some transactions (or commands) may demand that the user re-confirms their identity before the transaction (or command) can be executed
  - They should be defined to RACF with the REVERIFY option
    - RDEFINE TIMS *MYTRAN1* UACC(NONE) APPLDATA('REVERIFY')
  - Set IMSPBxxx RVFY=Y
  - The user would enter his or her password in an MFS non-display field
  - The input message composed by MFS would be like –
    - MYTRAN1(*user_password*) *transaction_data*
    - /DBR(*user_password*) DATABASE *db_name*

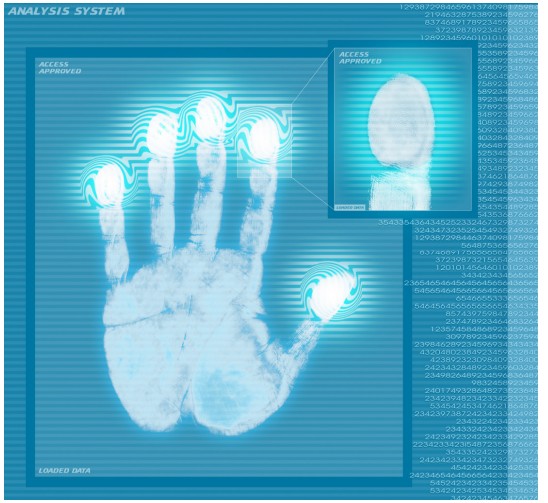
Security Auditing

Security Auditing

- **When security is important, a key role is that of the Security Auditor**
  - RACF allows the security auditor to control what activities gets audited
- **RACF uses SMF (dataset or log stream) to record audited activity**
  - And provides tooling for post-processing the collected data
- **IMS authorisation calls to RACF always (since IMS 10) request auditing**
  - RACROUTE REQUEST=FASTAUTH,**LOG=ASIS**
- **IMS also maintains a security audit trail on the IMS log**
  - Failed SIGN ON in X'10' log record
  - Successful SIGN ON (and OFF) in x'16' log record
  - Userid is logged in message and DB Update log records
- **Security Violations can cause an alert to be raised**
  - RACF sends message to its Security Console (sign on or authorisation failure)
  - RACF can also notify a TSO ID (as specified in profile of each individual resource)
  - IMS can also notify MTO
    - If **`SECURITY SECCNT=1|2|3`**
      - **`SECCNT=0`** → no MTO notifications

And Finally …

What hasn't been covered



- **Physical Security**
  - Key pads, retinal scans, etc. etc, etc.
- **Encryption and SSL (for IMS Connect)**
- **Shared Queues Structure Security (for access by IMS and by CQS)**
- **Application-based security**
  - AUTH call

- **Special cases**
  - Static ISC Links
- **RESUME TPIPE alt_client security**
- **CICS DBCTL, ODBA and APPC CPI-C use of PSBs**
- **Additional security for /LOCK, /UNLOCK, and /SET**
- **VSAM Passwords**
  - For stand-alone batch applications
- **……**

Summary

- **RACF can be used to provide a full security implementation with IMS**
- **It is up to you to –**
  - Choose the security facilities appropriate to your needs, determine the best way to implement each facility, and do the implementation
- **Some security facilities are obvious basic choices**
  - Dataset Access, Sign on, Transaction and Command authorisation, RAS, ….
- **Others enable even tighter controls to be maintained**
  - TERMINAL security, Connection security, DBRC security, Structure security, …
- **RACF offers many options for further enhancing security**
  - PROTECTED and RESTRICTED attributes, selected notification of violations, REVERIFY option, Mixed case passwords, PassTickets, “Catch All” generic profiles, …
- **IMS too, has many choices to be made**
  - Forced Sign-On for Static terminals? What userid to use for AOI command calls? How to handle MSC Link Receive security? How to implement security for end-users who have no userid? What ACEE ageing value to set for OTMA? Are Security Exits needed? …

Make the right choices, and what you get is **ROCK SOLID** ***Security***