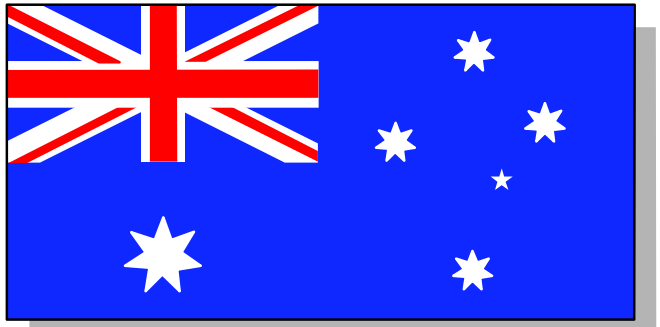
Implementing DFSCCMD0 to enhance IMS Command Security

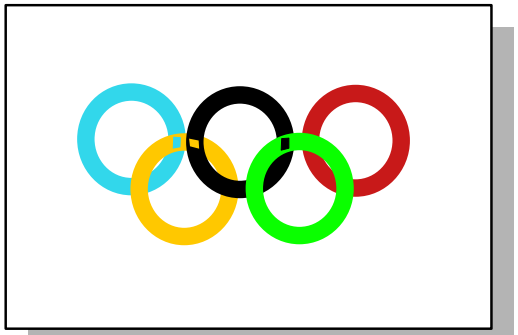
A User's Perspective

RETURN TO INDEX

IMS Technical Conference, 2000
Session E49

Robert Hain,
IBM Global Services Australia.





Topics in today's presentation:

- Background to our environment
- Why did we need better security?
- What did we want to end up with ?
- Info about DFSCCMD0
- Initial implementation under IMS V5
- What changed with IMS V6
- Roll-out & implementation
- Further enhancements
- Current Status
- Where to next.

The Telstra Environment

- Until November 1997, 100% Government owned telephone company.
- Partially floated since 1997.
- Mainframe Computer sites in Melbourne and Sydney.
- IMS Used for several applications, predominantly the billing system.
- 32 IMS systems (5 Production systems)

IMS Front-end Systems

- **Online billing system :**
  - 7-10 million transaction / day
  - Predominantly DB2 data (some IMS FF DBs)

IMS Back-end System

- **Itemised call information**
  - About 10% of online transactions from front-end system via MSC link
  - Mainly BMPs
  - About 5,500 DEDB areas (4 terabytes data)
  - Logs 136Gb data / day
    - (Averaging 1.8Mb / second over 24 hours)

History of IBM GSA & Telstra

- Until July 1997, Telstra managed it's own IT
  - IMS Support staff belonged to Telstra
  - IMS DBA staff belonged to Telstra

History (cont.)

- July, 1997 Telstra out-sourced operations to a newly formed company IBM GSA
  - 51% owned IBM Australia
  - 33% owned Telstra
  - 16% owned Lendlease

History (cont.)

- Changed dynamics of the relationship between IMS Systems Programmers and DBAs
- Systems Programmers now belong to IBM GSA
  - DBAs still owned by Telstra
  - Working together, via a contract
    - different management
    - different company
    - different objectives

IMS Command Security

- Refer to :
  - IMS manuals
  - Security Redbook (SG24-5363-00)
  - Lonie Coleman's presentation E45

IMS Command Security (cont.)

- IMS Stage 1 :
  - SECURITY MACRO
    - RCLASS=xxx
      - Will refer to RACF classes Cxxx & Dxxx
    - TYPE=RACFCOM
      - Specifies RACF security to be used for commands
- DFSPByyy member
  - RCF=C
    - Can override the RACFCOM in the gen

IMS Command Security (cont.)

- RACF class CIMS (if RCLASS=IMS)
- Can specify access to any specific command
- RACF class DIMS (if RCLASS=IMS)
  - Can group commands together into different profiles
  - Provide access to a group of commands in a single profile
- Telstra only uses DIMS

IMS Command Security (CIMS)

```
CLASS      NAME
-----      ----
CIMS       ** (G)

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

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
 -----     --------          ---------------          ----------          -------
 00      SECIMS             NONE                NONE          NO

RESOURCE GROUPS
-------- ------
NONE

USER      ACCESS
----      ------
NO USERS IN ACCESS LIST

  ID     ACCESS  CLASS             ENTITY NAME
-------- ------ -------- --------------------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST
```

IMS Command Security (DIMS)

```
CLASS      NAME
-----      ----
DIMs       DBA

MEMBER CLASS NAME
------ ----- ----
CIMS

RESOURCES IN GROUP
--------- -- -----
DBD
DBR
MOD
STA
STO
SWI

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ---------------  -----------  -------
 00    RACFADMN       NONE             NONE     NO
USER      ACCESS   ACCESS COUNT
----      ------   ------ -----
QPIMS     READ       000000
```

IMS Command Security - ICMD calls

- Any CMD calls will use SMU security.
- Any ICMD calls will refer to AOIS startup value
  - AOIS=R
    - RACF authorisation for commands entered via ICMD calls in programs

IMS Command Security - MCS consoles

- Any MCS console command will refer to CMDMCS startup value
  - CMDMCS=R
    - RACF authorization for commands entered via MCS consoles

Our problem !

- RACF Command security only at the command level.
- Too many commands had many keywords
- IMS Support (IBM GSA) required access to some
- DBAs (Telstra) required access to others
  - ie. /STA REG, /STA DB

How it had to end up (security perspective)

- All security should use RACF
- Any user written security rules /profiles should start with "$"

How it had to end up (IMS perspective)

- Needed command and 1st keyword
- Continue using CIMS/DIMS
  - Single point of validation
- Profile to contain command & keyword.
- Decided on $ccckkk
  - $: due to secuity requirement
  - ccc : 3 digit command string
  - kkk : 3 digit keyword string

A little about DFSCCMD0

- Command Authorization Exit
- Uses Callable Services
- Sample provided by IMS uses an internal table to check access
  - not easily maintainable
  - we need different rules on different systems
- Didn't use RACF

A little more about DFSCCMD0

- Exit gets control :
  - After standard command validation
    - RACF
    - SMU
  - Before any command syntax checking

Invoking DFSCCMD0

- Placing the exit into RESLIB, will automatically invoke it for any terminal user
- AOIS=A
  - for ICMD call users
- CMDMCS=B
  - for MCS console users
- APPCSE=C or F
  - for APPC users

Initial logic with IMS Version 5

- Only catered for terminal entered commands
- Had access to the RACF ACEE via the CTB
- Parsed the command string to obtain the 1st keyword.
- Created string for validation ($ccckkk)

What changed wth IMS V6

- Before we knew it, we were implementing IMS V6
- Decided to use MCS console support
- Prepare for ICMD usage

MCS consoles & RACF

- Following V6 implementation, new automation package was to use MCS console support to communicate with IMS.
- MCS Console users do not have a userid !
- IMS assumes the MCS console name to be the userid.

MCS consoles ...

- Had to
  - defined RACF userids the same as the consoleid.
  - Discuss with security how secure the use of consoles was.

Changed specs for DFSCCMD0

- Expanded the logic to include :
  - MCS console support
  - ICMD call support

but .....

- DFSCCMD0 was written assuming the RACF ACEE could be obtained from the CTB
- MCS Console users do not have a CTB or RACF ACEE !
- ICMD call users do not have a CTB or RACF ACEE !
- Need a RACF ACEE to issue a RACF call !

Back to the drawing board !

DFSCCMD0 Version 2

- Had to use RACF to :
  - build an ACEE
  - use the ACEE
  - delete the ACEE
- Larger chance of error
  - more getmain / freemain requests
  - far more complex code

Command acronyms

- Any 1 keyword could have many valid acronyms
- Altered code to use the IMS Keyword Table (DFSCKWD0)
- Use the internal IKEY value for RACF validation
  - Not documented anywhere
  - Need to refer to the source

DFSCKWD0 documentation

Table 14. Keywords, Synonyms, and Their Environments

Keyword	Synonym	DB/DC	DBCTL	DCCTL
ABDUMP		X	X	X
ABORT		X	X	X
ACCESS		X	X	
ACTIVE	A, ACT	X	X	X
ADS		X	X	
AFFINITY	AFFIN, AFF	X		X
AOITOKEN	AOITKN	X	X	X
APPC		X		X
AREA		X	X	
ASR		X		X
ASSIGNMENT	ASMT	X		X

DFSCKWD0 doc (cont.)

QCNT		X		X
QMGR		X		X
QUIESCE		X		X
RDR		X		X
READY		X		X
REGION	REGIONS, REG, REGS, MSGREG, MSGREGS, MSGREGION, MSREGIONS, THREAD	X	X	X
REMOTE		X		X
RESET		X	X	X
RTCODE	RTC, RCS	X		X
SB		X	X	
SEGNO		X		X

DFSCKWD0

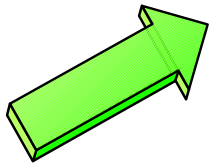
```
IKEY     REG
DFSCMDFL DBTM=Y,DBCT=Y,DCCT=Y
DFSCMDRL ACTV=Y,XALT=Y
KEYWD    REGION
SYN      REG
SYN      REGS
SYN      REGIONS
SYN      MSGREG
SYN      MSGREGS
SYN      MSGREGION
SYN      MSGREGIONS
SYN      THREAD
```

RACF Profiles

```
CLASS      NAME
-----      ----
DIMFD      DBA

MEMBER CLASS NAME
------ ----- ----
CIMFD

RESOURCES IN GROUP
--------- -- -----
$DBD* (G)
$DBR* (G)
$MOD* (G)
$STAARE
$STADAT
$STADGR
$STAPRO
$STATRA
$STOADS
$STOARE
$STODAT
```



```
$STADGR
$STAPRO
$STATRA
$STOADS
$STOARE
$STODAT
$STODGR
$STOPRO
$STOTRA
$SWIOLD
DBD
DBR
MOD
STA
STO
SWI
```

Rollout & Implementation

- Tested
- Installed in Development for ~6 months
- Reworked exit over many months
- Improved on syntax checking.
- Installed into Production

CRASH !

- Someone entered a command syntactically incorrect
- IMS crashed !
- Backed out immediately

Testing

- Testing is critical
- Improved testing.
- TPNS creating random string of command and keywords

Current Status

- Exit has been reworked, now sitting in all dev systems again
- Still undergoing testing
- Hope to reach production early 2001.

Wouldn't it be nice if .....

- IMS had a generalized command parsing routine
  - How many exits need to parse an IMS command string ?
- Callable services had a RACF option

Further Reading

- IMS V6 Security Redbook
  - SG24-5363-00

Any questions.