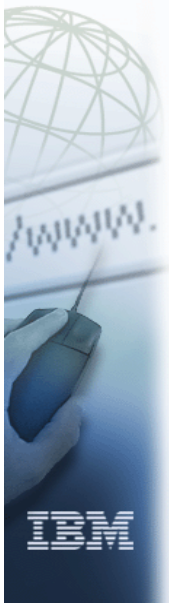


ibm.com



Multilevel Security z/OS Version 1 Release 5



Redbooks
International Technical Support Organization



© Copyright IBM Corp. 2004. All rights reserved.

Trademarks



eNetwork	DFSMS/MVS	IMS	RACF
geoManager	DFSMSdfp	IMS/ESA	RMF
AD/Cycle	DFSMSdss	IP PrintWay	RS/6000
ADSTAR	DFSMSshm	IPDS	S/390
AFP	DFSMSrmm	Language Environment	S/390 Parallel Enterprise Server
APL2	DFSORT	Multiprise	SecureWay
APPN	Enterprise System 3090	MQSeries	StorWatch
BookManger	Enterprise System 4381	MVS/ESA	Sysplex Timer
BookMaster	Enterprise System 9000	Network Station	System/390
C/370	ES/3090	NetSpool	SystemView
CallPath	ES/4381	OfficeVision/MVS	SOM
CICS	ES/9000	Open Class	SOMobjects
CICS/ESA	ESA/390	OpenEdition	SP
CICS/MVS	ESCON	OS/2	VisualAge
CICSPlex	First Failure Support Technology	OS/390	VisualGen
COBOL/370	FLowMark	Parallel Sysplex	VisualLift
DataPropagator	FFST	Print Services Facility	VTAM
DisplayWrite	GDDM	PrintWay	WebSphere
DB2	ImagePlus	ProductPac	3090
DB2 Universal Database	Intelligent Miner	PR/SM	3890/XP
DFSMS/MVS	IBM	QMFr	z/OS
			z/OS.e

Domino (Lotus Development Corporation)
DFS (Transarc Corporation)
Java (Sun Microsystems, Inc.)
Lotus (Lotus Development Corporation)

Tivoli (Tivoli Systems Inc.)
Tivoli Management Framework
(Tivoli Systems Inc.)
Tivoli Manger (Tivoli Systems Inc.)

UNIX (X/Open Company Limited)
Windows (Microsoft Corporation)
Windows NT (Microsoft Corporation)

© Copyright IBM Corp. 2004. All rights reserved.

Multilevel Security (MLS)



- ❑ Valuable to commercial customers
 - Can set up a small set of SECLABELs and few SETROPTS options:
 - MACTIVE and SECLABELCONTROL
- ❑ Example: MVS system with HTTP Server
 - Assign a “low” SECLABEL to external customers so they can access “external” data
 - Assign a “high” SECLABEL to employees so they can access both “internal” and “external” data
- ❑ MLS option helps prevent declassification of data
 - SETROPTS CLASSACT(MLS)

© Copyright IBM Corp. 2004. All rights reserved.

Required Software for MLS



- ❑ z/OS V1R5
- ❑ RACF component - Security Server optional feature
- ❑ For backing up and restoring z/OS UNIX files:
 - DFSMSDss
- ❑ To implement system-specific security labels:
 - JES2 V1R5
- ❑ For secure printing:
 - Print Services Facility (PSF)
 - Overlay Generation Language/370 (OGL)
- ❑ DB2 V8 - can enable a single repository of data to be managed at the row level and accessed by individuals based on their need to know

© Copyright IBM Corp. 2004. All rights reserved.

Components added or extended functions to support Multilevel Security



☐ z/OS 1.5 key additions

- RACF
- UNIX System Services
- zFS
- TCP/IP
- JES2 (not JES3)
- SDSF
- DFSMS - MLS SECLABELs in ACS Routines
- DB2 V8
 - Security labels on rows in tables
 - See: <http://www-3.ibm.com/software/data/db2/os390/db2zosv8.html>

"Planning for Multilevel Security" has a complete list

© Copyright IBM Corp. 2004. All rights reserved.

Resource Candidates for SECLABELs



- ☐ Data sets
- ☐ User IDs
- ☐ UNIX files
- ☐ Console operator
- ☐ JES2 checkpoint data sets
- ☐ JES2 spool data sets
- ☐ JES2/JES3 started procedure
- ☐ OMROUTE
- ☐ RACF started procedure
- ☐ Security administrator
- ☐ SYSLOG daemon
- ☐ TCP/IP stack
- ☐ NETACCESS profiles (for IP addresses)
- ☐ STACKACCESS profiles
- ☐ XCF couple data sets

© Copyright IBM Corp. 2004. All rights reserved.

Multilevel Security



- ❑ Multilevel security is a security policy that allows:
 - Classification of data and users based on:
 - Hierarchical security levels combined with
 - Non-hierarchical security categories
- ❑ Multilevel-secure security policy has two primary goals, as follows:
 - First, the controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization
 - Second, the controls must prevent individuals from declassifying information

© Copyright IBM Corp. 2004. All rights reserved.

Mandatory Access Control (MAC)



- ❑ A MAC check compares the security labels of the subject and object and grants the subject access to the object
 - A subject can read an object if the subject's security label dominates the object's security label
 - A subject can write to an object if the object's security label dominates the subject's security label
 - A subject cannot write to an object whose security label the subject's security label dominates, unless the security labels are equivalent - not allowed to write down
 - A subject can both read and write an object only if the subject's and object's security labels are equivalent

© Copyright IBM Corp. 2004. All rights reserved.

Discretionary Access Control (DAC)



- ❑ Once the user passes a MAC check, a discretionary check follows
- ❑ A DAC check ensures that the user is identified as having a "need to know" for the requested resource
 - DAC uses other access control information, such as:
 - Access control list in the profile protecting a resource
 - z/OS UNIX access control (permissions, the access control list, and the UNIXPRIV class)

MAC check occurs first, then DAC
Or DAC only, if the SECLABEL class is not active

© Copyright IBM Corp. 2004. All rights reserved.

Multilevel Security and MAC



- ❑ Classifies data using
 - Security Levels
 - Security categories
- ❑ System controls access to resources
 - Labels resources
 - Enforces accountability
 - Prevents 'declassifying' data
 - Does not allow reuse of data objects until purged

© Copyright IBM Corp. 2004. All rights reserved.

SECLABELs and MAC



SETROPTS CLASSACT(SECLABEL) RACLIST(SECLABEL)

- ☐ PURPLE could be a SECLABEL name indicating SECLEVEL secret for categories PROJECTA, PROJECTB, and PROJECTC
- ☐ GREEN could be a SECLABEL name indicating SECLEVEL sensitive for categories PROJECTA and PROJECTB
- ☐ RED could be a SECLABEL name indicating SECLEVEL unclassified for category PROJECTC

SECLABEL	SECLEVEL	CATEGORY (Not required)
PURPLE	SECRET	PROJECTA, PROJECTB, PROJECTC
GREEN	SENSITIVE	PROJECTA, PROJECTB
RED	UNCLASSIFIED	PROJECTC

© Copyright IBM Corp. 2004. All rights reserved.

Defining SECLABELs



- ☐ Create SECDATA profiles

```
RDEFINE SECDATA SECLEVEL UACC(NONE)
RALTER SECDATA SECLEVEL
ADDMEM(seclevel-name/seclevel-number)
```

```
RDEFINE SECDATA CATEGORY UACC(NONE)
RALTER SECDATA CATEGORY
ADDMEM(category-1 category-2 ...)
```

© Copyright IBM Corp. 2004. All rights reserved.

Special SECLABELs and Definitions



- ❑ SYSHIGH
- ❑ SYSLOW
- ❑ SYSNONE
- ❑ SYSMULTI - (New with MLS in z/OS V1R5)
- ❑ Defining SECLABELs

RDEFINE SECLABEL security-label

SECLEVEL(seclevel-name)

ADDCATEGORY(category-1 category-2 ...)

PERMIT security-label CLASS(SECLABEL)

ACCESS(READ) ID(user-id-1 user-id-2 ...)

SETROPTS CLASSACT(SECLABEL)

RACLIST(SECLABEL)

or

SETROPTS RACLIST(SECLABEL) REFRESH

© Copyright IBM Corp. 2004. All rights reserved.

SYSMULTI SECLABEL



- ❑ SYSMULTI
 - Compares as "equivalent" to any other defined SECLABEL for MAC decisions
 - Intended for daemons and servers that can accept connections from users running at different classification levels (SECLABELs) and properly mediate data access
 - UNIX directories (often, not always, root in a file system) that can have subdirectories of different SECLABELs

© Copyright IBM Corp. 2004. All rights reserved.

SECLABEL by System



- ❑ Share a RACF database between systems and isolate use of specified SECLABELs to specified systems
- ❑ Specified by a member list on a SECLABEL profile
 - No members listed
 - Usable anywhere
 - Members listed
 - Usable only on one of those systems
- ❑ Not applicable to the SECLABELs provided by RACF,
 - SYSHIGH, SYSLOW, SYSNONE, SYSMULTI
- ❑ Enabled via the new SETROPTS option SECLBYSYS or NOSECLBYSYS

© Copyright IBM Corp. 2004. All rights reserved.

SECLABEL by System Example



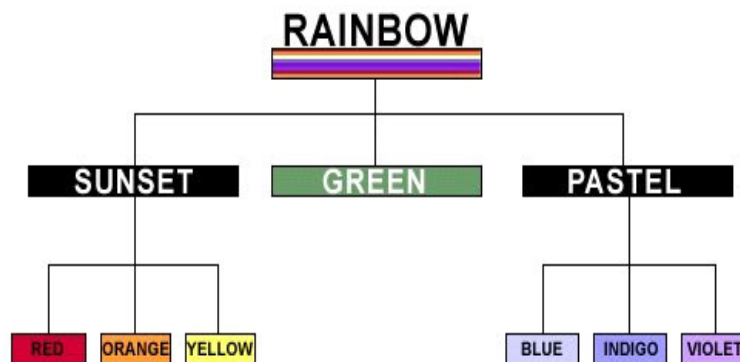
- ❑ SECLABELs A, B, and C with Systems SYS1 and SYS2
- ❑ Administrator could define them as follows:
 - RDEF SECLABEL (A,B) ... ADDMEM(SYS1)
 - RDEF SECLABEL C ... ADDMEM(SYS2)
- ❑ Then any attempt to access system SYS1 using SECLABEL C, or any attempt from SYS1 to access resources with SECLABEL C would fail
- ❑ Any attempt to access system SYS2 using SECLABEL A or B, or any attempt from SYS2 to access resources with SECLABEL A or B, would fail

© Copyright IBM Corp. 2004. All rights reserved.

SECLABEL Hierarchy

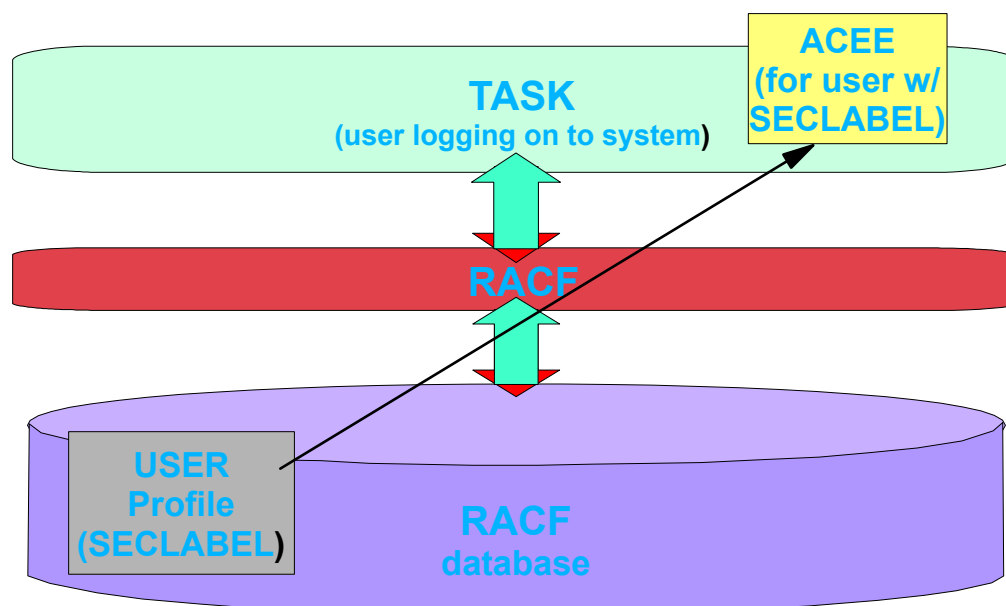


- For SECLABEL A to dominate SECLABEL B
 - The Security Level of A is equal to or greater than the Security Level of B
 - A has at least all the categories that define B



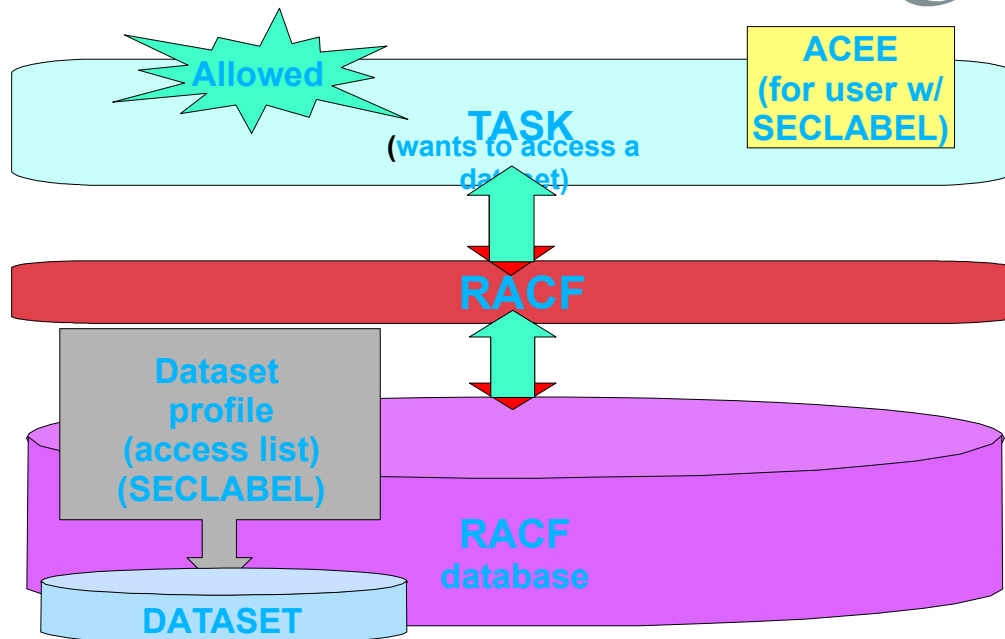
© Copyright IBM Corp. 2004. All rights reserved.

MAC Scenario (user logon)



© Copyright IBM Corp. 2004. All rights reserved.

MAC Scenario (access attempt)



© Copyright IBM Corp. 2004. All rights reserved.

SECLABEL Processing Summary



- ❑ By activating the SECLABEL class and RACLISTing it, SECLABEL processing is active
 - SETR CLASSACT(SECLABEL) RACLIST(SECLABEL)
- ❑ First MAC, then DAC is done if both user and object has a SECLABEL
- ❑ Only DAC is done, if user has a SECLABEL and object does not have a SECLABEL
- ❑ Authority testing fails if object has SECLABEL, but user does not have a SECLABEL
- ❑ Should not happen often since user cannot easily logon without a SECLABEL if the SECLABEL class is active.

© Copyright IBM Corp. 2004. All rights reserved.

Restrictions for Shared DASD



- ❑ If your system is a shared DASD environment (multiple MVS systems sharing workload and DASD)
 - All z/OS systems must have z/OS V1R5 or higher
 - All z/OS systems must share the RACF database in order to make identical security decisions
 - The z/OS systems in the global resource serialization complex must be the same set of z/OS systems that are sharing the RACF database
 - The JES complex (JES2 MAS or JES3 complex) must be either the same set of z/OS systems that share the RACF database, or a subset of these systems

© Copyright IBM Corp. 2004. All rights reserved.

New Support for z/OS Components



- ❑ SECLABELs for z/OS UNIX processes and sockets
- ❑ SECLABELs for z/OS UNIX files and directories
- ❑ SECLABELs for z/OS UNIX interprocess communications
- ❑ SECLABEL by system
 - RACF SECLBYSYSTEM option
- ❑ zFS supports security labels for MLS
 - Externals for MLS are contained in other elements/components
 - (RACF, shell, z/OS UNIX APIs, etc.)
 - zFS supports low level functions for MLS

© Copyright IBM Corp. 2004. All rights reserved.

Multilevel Security with z/OS V1R5



- ❑ Support is added allowing SECLABELs to be associated with file system resources and users to provide greater restrictiveness than is possible with POSIX permissions alone
 - ALL systems must be z/OS V1R5
 - Requires use of zFS for ROOT and /dev resources
 - Requires use of zFS for all file systems mounted for readwrite access

© Copyright IBM Corp. 2004. All rights reserved.

Summary



- ❑ Hardware - Must run z/OS V1R5
- ❑ Software - z/OS V1R5
 - RACF
 - For System specific security labels-- JES2
 - Print Services Facility (PSF)
 - Overlay Generation Language/370-or alternate
- ❑ Sysplex (shared DASD) constraints
 - All systems must be at z/OS V1R5 or higher
 - All systems must share the RACF database
 - All systems in the GRS complex must be the same as those in the RACF Database
 - JES complex must be the same
- ❑ Not supporting multilevel security
 - Infoprint Server and BDT
 - Partial support
 - See "Planning for Multilevel Security"

© Copyright IBM Corp. 2004. All rights reserved.