



IBM Systems Group

Introduction to Multilevel Security (MLS)

RACF-2004
Session D5
June 2004

Mark Nelson, CISSP
z/OS Security Server (RACF) Design and Development
IBM Poughkeepsie
markan@us.ibm.com

Agenda

- **What is Multilevel Security?**
- **The Road to Multilevel Security**
- **Levels and Categories**
- **SECLABELs**
- **Dominance and Equivalence**
- **Discretionary vs. Mandatory Access Controls**
- **Controlling Multilevel Security using SETROPTS**
- **Considerations**

Trademarks

- **The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:**
 - ▶ IBM
 - ▶ RACF
 - ▶ z/OS, OS/390, MVS
 - ▶ zSeries

- **Other company, product or service names may be trademarks or service marks of others.**

What is Multilevel Security?

- **Multilevel security is:**

- ▶ The ability to mix different categories and classes of information within the same computing environment in a controlled manner without compromise
- ▶ A combination of hardware, software, and operational procedures
- ▶ Valuable anytime there is a need to isolate data, such as:
 - In a service bureaus environment
 - When there is truly sensitive data
 - As a way of complying with evolving regulatory environment

The Road to Multilevel Security

- **RACF's support for multilevel security has evolved since the mid-80s:**
 - ▶ 1985: RACF 1.7 - Assignment of levels and categories to users and data objects
 - ▶ 1990: RACF 1.9 - Multilevel ("B1") support
 - SECLABELs
 - Console logon
 - NJE, RJE, JES controls
 - No support for TCP/IP, DB2
 - ▶ 2004: z/OS R5 – Multilevel support
 - Extends existing multilevel controls to TCP/IP, UNIX System Services, and DB2

The Road to Multilevel Security...

■ 1985/RACF 1.7: Levels and Categories:

- ▶ **Security level (SECLEVEL), a hierarchical classification ('PUBLIC', 'INTERNAL USE', 'CONFIDENTIAL', 'TOP SECRET')**
- ▶ **Security category, a non-hierarchical classification ('HR', 'RESEARCH', 'FINANCIAL', 'ICE NINE')**
- ▶ **Levels and categories are assigned to users and data objects**
 - When a user access a resource which has a SECLEVEL or security category, the user must have a higher SECLEVEL and all of the categories that are associated with the resource.
- ▶ **SECLEVELs and categories are defined in the SECDATA general resource class**

```
RALTER SECDATA SECLEVEL ADDMEM('UNCLASSIFIED'/10,  
    'CONFIDENTIAL'/20, 'SECRET'/30, 'ULTRA'/100)
```

```
RALTER SECDATA CATEGORY ADDMEM(FINANCIAL HR RESEARCH)
```

Why Multilevel Security

- **Traditional access control mechanisms allow the resource owner to control who has access to data**
 - ▶ The data owner has the discretion to grant access, hence the term 'discretionary access' mechanism.

- **Data classifications, if present are assigned by the data owner**
 - ▶ Data owners could misclassify data by opening a data set at one level and then writing it to another level

- **Multilevel security formalizes the classification of data and enforces a data access policy that is set by the security administrator, not the data owner**

RACF and Multilevel Security: The SECLABEL

- **MVS 3.1.3 and RACF 1.9 (1990) introduced the concept of the security label or SECLABEL**
- **A security label or SECLABEL consists of two parts:**
 - ▶ A security level (SECLEVEL)
 - ▶ Zero or more security categories
- **SECLABELs are defined in the SECLABEL class**

```
RDEFINE SECLABEL PUBINFO  SECLEVEL(UNCLASSIFIED)  ADDCATEGORY(FINANCIAL HR RESEARCH)
RDEFINE SECLABEL HRCONF   SECLEVEL(CONFIDENTIAL)  ADDCATEGORY(HR)
RDEFINE SECLABEL EXECUTIV SECLEVEL(ULTRA)         ADDCATEGORY(FINANCIAL RESEARCH HR)
```


RACF and Multilevel Security: The SECLABEL...

- **In a fully-operational multilevel security environment, all users and data objects must have SECLABELS**
- **SECLABELS can be assigned to users (including started task and batch users), data resources, and to other security-related objects (such as terminals) using RACF commands:**

```
ADTDSD 'PERSONEL.EMPLOYEE.DATA' SECLABEL(HRCONF)
```

```
ALTUSER MARKN SECLABEL(EXECUTIV)
```

RACF and Multilevel Security: The SECLABEL...

- **RACF provides several system-defined SECLABELs:**
 - ▶ **SYSHIGH:** The highest defined SECLEVEL and all defined categories
 - ▶ **SYSLOW:** The lowest defined SECLEVEL and no defined categories
 - ▶ **SYSNONE:** Assigned to resources which do not contain data, such as catalogs

- **The SECLABEL class must be RACLISTed**

RACF and Multilevel Security: The SECLABEL...

- **Assigning a SECLABEL to a user does not give the user access to the SECLABEL; The user must be PERMITTED to the SECLABEL:**

```
PERMIT EXECUTIV CLASS(SECLABEL) ID(MARKN) ACCESS(READ)
```

Dominance and Equivalence

- **When SECLABELs are compared in an access check, RACF examines the dominance relationship between the SECLABELs.**
 - ▶ 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**
 - Avoid the temptation to say that SECLABEL **A** is “greater” than SECLABEL **B**
- **SECLABELs A and B are equivalent if the A dominates B and B dominates A**
 - ▶ Same SECLEVEL
 - ▶ Same set of categories
 - ▶ Equivalence is a ‘subset’ of dominance
- **Disjoint SECLABELs are SECLABELs where there is at least one category in SECLABEL A that is not in SECLABEL B and one category in SECLABEL B that is not in SECLABEL A**

Discretionary vs. Mandatory Access

■ **Discretionary Access Control**

- ▶ “A means of restricting access to objects based upon the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject”

■ **Mandatory Access Control**

- ▶ “A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity,”

Discretionary and Mandatory Access Check

- **Discretionary Access Checks (DAC) and Mandatory Access Checks (MAC) work together:**
 - ▶ Mandatory checks are performed first
 - ▶ If the mandatory check passes, then the discretionary access checks are performed
 - Access list
 - UACC
 - Etc.

SECLABEL Relationship for Processing Data

- **In a fully operational MLS environment:**
 - ▶ Reading data requires that the subject's SECLABEL must dominate the object's SECLABEL
 - ▶ Writing data requires that the object's (data) SECLABEL must dominate the subject's (user's) SECLABEL
 - ▶ Reading and writing data requires that the object's SECLABEL must be equivalent to the subject's SECLABEL

- **SETROPTS options control exactly how robust you want your MLS environment to be**

Reverse Mandatory Access Checking

- **For some types of objects the required dominance relationship is 'opposite' of a normal dominance relationship**
 - ▶ Reading data requires that the object's SECLABEL dominates the subject's SECLABEL
 - ▶ Reading and writing data requires that the object's SECLABEL is equivalent to the subject's SECLABEL
 - ▶ These types of objects have RVRSMAC=YES in the RACF Class Descriptor Table (CDT)

SECLABEL-related SETROPTS Controls

- **The SETROPTS command is used to control the enabling of multilevel security controls through the use of these SETROPTS options:**
 - ▶ SETROPTS CLASSACT(SECLABEL)
 - ▶ SETROPTS MLACTIVE
 - ▶ SETROPTS MLSTABLE
 - ▶ SETROPTS MLQUIET
 - ▶ SETROPTS SECLABELCONTROL
 - ▶ SETROPTS COMPATMODE

Activating SECLABEL Processing

- **Activating and RACLISTing the SECLABEL class activates SECLABEL processing**
 - ▶ **SETR CLASSACT(SECLABEL) RACLIST(SECLABEL)**
- **This alters the access check path:**
 - ▶ If the both the user and the object have a SECLABEL then the user's SECLABEL is compared to the resource
 - ▶ If the resource has a SECLABEL and the user does not, then the access check fails.
 - ▶ If the user has a SECLABEL and but the resource does not, then the access check continues with the discretionary access check.

SETROPTS MACTIVE

- **With MACTIVE, RACF requires that all resources for classes with SECLABEL=REQUIRED in the CDT have SECLABELs**
- **This option is activated by issuing the command:**
 - ▶ **SETR MACTIVE**
- **There are WARNING and FAILURE modes for this option**

SETROPTS MLS

- **With SETR MLS in effect, RACF enforces the write-down property**
 - ▶ Subjects are prevented from writing down to a “lower” SECLABEL
 - ▶ Sometimes called the “*-property”

- **Prevents improper declassification of data**
 - ▶ Reading data requires that the subject(user) must dominate the object’s SECLABEL
 - ▶ Writing data requires that the object’s SECLABEL must dominate the subject SECLABEL
 - ▶ Reading and writing data requires that the SECLABEL of the subject and the SECLABEL of the object are equivalent

SETOPTS MLS...

- **This option is activated by issuing the command:**
 - ▶ **SETR MLS**

- **There are WARNING and FAILURE modes for this option**

- **When SETR NOMLS (MLS is of) is in effect:**
 - ▶ Reading or reading and writing data requires that the subject(user) dominates the object's

 - ▶ Writing data requires that the subject's SECLABEL dominates the user's SECLABEL or the object's SECLABEL dominates the user
 - SECLEVELs may be different, but the categories must match!

SETROPTS MLS/MLACTIVE WARNING Mode

- **If either MLS and/or MLACTIVE are in warning mode, RACF will pass a MAC test and generate warning message (ICH408I) if:**
 - ▶ The request would have passed if the option was off
 - ▶ The request will fail with the option on

- **This can be done by placing WARING after the SETROPTS MLS or MLACTIVE:**
 - ▶ **SETR MLS (WARNING)**
 - ▶ **SETR MLACTIVE (WARNING)**

- **This may be something useful when first enabling MLS or MLACTIVE to ensure all the correct profiles have been created with the correct SECLABELS**

SETROPTS MLSTABLE

- **Ensures that SECLABELs won't change while someone is in the process of using them by:**
 - ▶ Preventing changes of SECLABELs definitions
 - ▶ Preventing changes of SECLABELs assigned to a RACF profile

- **Must set MLQUIET to allow such changes to occur while MLSTABLE is active**

SETROPTS MLQUIET

- **Allows changing of SECLABEL definitions and SECLABELs within a RACF profile**
- **Overrides (and only needed if) MLSTABLE is active**
- **Only SPECIAL, TRUSTED, or console operator can logon or access resources protected by RACF profiles.**

SETROPTS SECLABELCONTROL

- **Prevents non-SPECIAL users from setting or changing a resource SECLABEL**
- **Without SECLABELCONTROL, a user who can create or modify a RACF profile, can also modify the SECLABEL assigned to the profile**

SETROPTS COMPATMODE

- A migration mode that allows users running **WITHOUT** a **SECLABEL** to access resources protected by RACF profiles that **HAVE** a **SECLABEL** if the user could use that SECLABEL
- Applies only to applications that issue **RACROUTE REQUEST=VERIFY** to create the user **ACEE** without specifying any RACF 1.9.0 or later keywords

Considerations

- **Do not attempt to enable a multilevel security environment unless you have an accepted and well-defined data classification policy**
- **All authorization checks are bypassed for objects which match entries in the RACF global access table (GAC) that are defined with the requested access authority.**
- **If `MLS` and `MLACTIVE` are both in `FAIL` mode, then any user that has the `SPECIAL` attribute and is logged on with `SYSHIGH` is treated as though they are in `WARNING` mode**
 - ▶ Useful to know if you get into trouble

References

- **RACF Security Administrator's Guide**
 - ▶ Chapter 4 – Classifying User and Data
 - ▶ Appendix F – In the section called:
 - “Security Label Authorization Checking”
- **Planning for Multilevel Security**
- ... available on the web from the “Library” section of the RACF web page (www.ibm.com/eserver/zseries/zos/racf)



IBM Systems Group

Introduction to Multilevel Security (MLS)

RACF-2004
Session D5
June 2004

Mark Nelson, CISSP
z/OS Security Server (RACF) Design and Development
IBM Poughkeepsie
markan@us.ibm.com