Multilevel Security

SHARE Washington DC
Session 1736
August 2003

George Markouizos
RACF Development
Telephone: (845) 435-8563
e-mail: gmarkou@us.ibm.com

Table of Contents

What is Multilevel Security?

- Multilevel Security is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories.
- Characteristics of a multilevel-secure system:
  - Access controls
    - Mandatory Access Control (MAC)
    - Discretionary Access Control (DAC)
  - Accountability
    - Auditing
    - Identification and Authentication
  - Trusted Computing Base
    - Hardware
    - Software

Why Multilevel Security?

- Multilevel Security provides a way to segregate users and their data from other users and their data regardless of access lists, UACC, etc.
- Valuable to government agencies
  - Use of functions like name-hiding, write-down, *-property (no write-down)
- Valuable to commercial customers (i.e. service bureau)
  - Can be set up using a small set of SECLABELs and few SETROPTS options (MLACTIVE 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

History and Evolution

- ~1990
  - MVS/ESA 3.1.3 with RACF 1.9, TSO/E, JES, DFP, VTAM, PSF etc., passes formal B1 evaluation having met the criteria specified in the Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD.
- ~1996
  - Some new functions added to OS/390, such as UNIX, Extended Consoles, TCP/IP, “not designed for B1”.
- 2004
  - With z/OS V1R5 “B1” support is extended to cover these functions.

Existing B1 support (before z/OS V1R5)

- RACF and other evaluated system components support Security Labels (a.k.a. SECLABELs).
- SECLABELs have two components:
  - Level (a number in the range 1-255)
    - Unclassified/1
    - Sensitive/25
    - Confidential/50
    - Secret/100
  - List of Categories (0 or more named categories)
    - Green
    - Yellow, Orange
    - Yellow, Orange, Red

security level: An installation-defined name that corresponds to a numerical security level; the higher the number, the higher the security level.

security category: An installation-defined name corresponding to a department or area within an organization with similar security requirements.

security label (**SECLABEL**): An installation-defined name that corresponds to a specific RACF security level with a set of zero or more security categories. This is another term for sensitivity label.

Existing B1 support

- Special system-defined SECLABELs
  - **SYSNONE**
    - Combines the lowest Security Level and has NO Categories
  - **SYSLOW**
    - Combines the lowest Security Level and has NO Categories
  - **SYSHIGH**
    - Combines the highest Security Level and ALL Categories

Notes on SYSNONE:

•Should never be assigned to a user

-Useful for data that users of different SECLABELs must write to, when SETROPTS MLS (no-write-down) is in effect.

-Should ONLY be used for data the user does not write to directly; data whose access (for writing) is mediated by another program that will ensure no classified content is written.

Example: system catalogs

Notes on SYSLOW:

•Used for any data without a security classification, such as data IBM supplies as part of the installation package for the system.

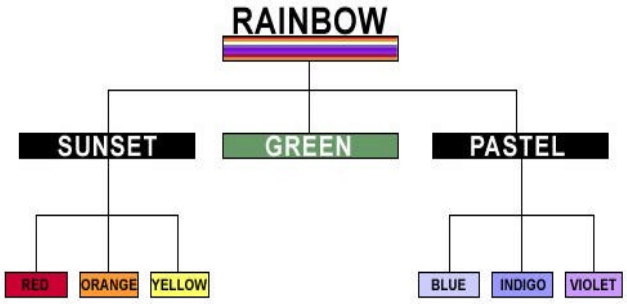
•Can also be used by customer for any data they create that has no need for classification.

Notes on SYSHIGH:

•Used for aggregation of data with a variety of SECLABELs, e.g.

- •system console (output from many jobs) until BCP supports segregating messages by SECLABEL
- •MVS system log (syslog)
- •UNIX syslog
- •Backup tapes if data not segregated on volumes or file systems by SECLABEL

SECLABEL Hierarchy



With the hierarchy established in the security manager layer, the system would understand that users with authority to read RAINBOW can read anything. Someone with authority to read PASTEL information can read any row associated with BLUE, INDIGO, VIOLET, or PASTEL. Someone with SUNSET can read SUNSET, RED, ORANGE, YELLOW. This is a lot more powerful than just having an exact match on SECLABEL (i.e., user's label must exactly match the data's label), since it has the notion of "groups" (in this case, sets of categories) that make security administration easier to manage.

See
http://www7b.boulder.ibm.com/dmdd/library/techarticle/0209cotner/0209cotner.html

Existing B1 support

- Each user has a default SECLABEL
- Some applications (TSO/E, batch jobs) support user requesting a specific SECLABEL
- Each port of entry (TERMINAL, card reader, ...) has a SECLABEL
- Each SECLABEL has a RACF profile
  - Access list
  - Universal access
  - Auditing information
- During user authentication, RACF validates user's requested SECLABEL
  - User must have access to that SECLABEL
  - SECLABEL must properly match the port of entry

Existing B1 support

- Various options to control such functions as
  - Whether users and resources must have SECLABELs or not
  - Whether write-down is allowed or not (system wide option)
  - How auditing should be performed
- Authorization checking:
  - User tries to access a resource
  - RACF compares resource SECLABEL with user's SECLABEL (MAC)
  - If that passes, RACF checks access list and universal access (DAC)
  - If that passes, RACF grants access

write-down - a.k.a. star-property or *-property implemented in RACF by the existing B1 MLS option

DAC – Discretionary Access Control

MAC – Mandatory Access Control

Some more granular definitions:

write-down: The action of an address space creating output data at a lower labeled classification than that at which the address space is executing

mandatory access control (**MAC**): A means of restricting access to objects on the basis of the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (clearance) of subjects to access information of such sensitivity

Existing B1 support

- Printer Support
  - Locally attached pagemode printers: 3800, 3900, 3130, ...
  - System can put a security classification on each page
  - Administrator can define "protected" areas of page where user cannot print
    - Administrator can allow selected users to override that restriction
  - System will only print on a printer if the SECLABEL assigned to the printer "**dominates**" the SECLABEL assigned to the output

dominate: One SECLABEL dominates a second SECLABEL when the security level that defines the first is equal to or greater than the security level that defines the second, and the set of security categories that defines the first includes the set of security categories that defines the second. A SECLABEL dominates itself since comparison of a SECLABEL with itself meets this definition.

z/OS V1R5 Multilevel Security enhancements

- New special system-defined SECLABELs
  - **SYSMULTI**
    - Used in cases where any classification of data could be "processed".
    - 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.
    - Generally should not be assigned to real users, nor to a server that is not designed to handle multiple SECLABELs.

SECLABELs and MAC checking

- Three types of MAC checking
  - MAC
    - User's current SECLABEL dominates Resource's SECLABEL
  - RVRSMAC (Reverse MAC)
    - Resource's SECLABEL dominates User's current SECLABEL
  - EQUALMAC (Equal MAC)
    - User's current SECLABEL is equivalent to the Resource's SECLABEL.
- New operand EQUALMAC= added on the ICHERCDE macro
  - EQUALMAC=YES
    - The class requires SECLABEL equivalence

Equivalence - Either the SECLABEL names are identical, or two different SECLABEL names that are defined with identical security level and categories. When determining equivalence, the SECLABEL SYSMULTI is considered equivalent to any SECLABEL

Disjoint security labels - Two security labels are disjoint when each of them has at least one category that the other does not have. Neither of the labels dominates the other.

SECLABELs for z/OS UNIX Processes and Sockets

- Currently TSO/E users:
  - Have the ability to select their current SECLABEL by specifying it on the logon panel, or they can use their default.
  - The value they enter is saved in the TSO segment and used as the default the next time they log on.
- This function has been modified to:
  - Handle workstations (allowing for both reading and writing)
  - Support the z/OS UNIX environment where a user may enter the system from a remote IP address using an application such as rlogin.
  - Associate SECLABELs to IP addresses.

Currently, when users enter the system through TSO/E they have the ability to select their current SECLABEL by specifying it on the logon panel, or they can use their default. The value they enter is saved in the TSO segment and used as the default the next time they log on. The SECLABEL of the terminal they are logging on to must dominate the user's SECLABEL.

This function has been modified to handle workstations (allowing for both reading and writing), the usage and characteristics of the TERMINAL class have changed to require SECLABEL equivalence and to supply the SECLABEL if none specified. The function has also been extended to support the z/OS UNIX environment where a user may enter the system from a remote IP address using an application such as rlogin.

The extension of SECLABELs to z/OS UNIX entails associating SECLABELs to IP addresses. Since the TERMINAL class cannot handle IP V6 addresses (due to their length), the usage and characteristics of the SERVAUTH class, which currently is used by the z/OS Communications Server (TCP/IP) to check server access authorization, have been changed so that IP V6 addresses can be accommodated.

SECLABELs for z/OS UNIX Processes and Sockets

- SERVAUTH class usage and characteristics have been enhanced to accommodate IP V6 addresses.
- New parameters have been added to InitACEE to allow the SECLABEL and SERVAUTH values to be passed.
- Corresponding changes have been made to allow applications to pass these values through UNIX System Services to InitACEE. These changes accommodate applications willing to change their code to allow the specification of a SECLABEL by the user.
  - New z/OS UNIX callable service, _poe, to set the port of entry for use by servers. Can set TERMINAL or SERVAUTH
  - z/OS UNIX Kernel will provide the server SECLABEL on the User Authentication call

The expanded usage of the SERVAUTH class requires a number of changes to its characteristics. Profiles in this class will require a SECLABEL if the MLACTIVE option is active. SECLABELs will be checked for equivalence rather than following the normal MAC authorization rules. Because it is a port of entry, changes to the SERVAUTH class can cause information to be removed from VLF, just as they can for TERMINAL and APPCPORT.

When the existing MLACTIVE option is set additional checking will be done by RACROUTE REQUEST=VERIFY and InitACEE to ensure that server applications do not allow users running with different security levels in the same server address space. When anchoring an ACEE in a TCB, where the address space already has an ACEE in the ASXB, the SECLABELs associated with each ACEE will be checked for equivalence. If they are not equivalent, the request will be failed with message ICH408I. Other products anchoring ACEEs in TCBs for client users should also ensure equivalence. Note that assigning SYSMULTI to the server address space indicates that the server allows clients at multiple security levels since SYSMULTI is equivalent to any defined SECLABEL.

For applications that do not allow the specification of a SECLABEL, a SECLABEL for the user must be derived from the user's port of entry; a resource in the SERVAUTH or TERMINAL class. TCP/IP, z/OS UNIX and RACF will work together to determine the SECLABEL associated with the IP address when the SECLABEL class is active, and associate it with the user's security environment if the user is authorized to use it.

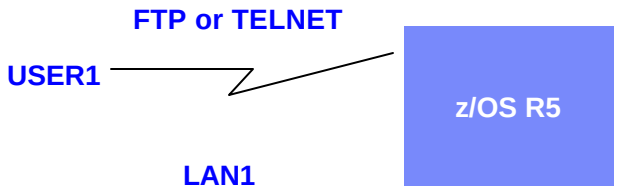
SECLABELs for z/OS UNIX Processes and Sockets

- Administrator can define IP subnetworks via RACF profiles
  - SERVAUTH class
  - Any granularity desired, down to individual IP address if needed
- SERVAUTH profile contains SECLABEL for that subnetwork
  - Customer responsible for network topology and protection of network links
    - IPSEC (VPN) can also be used to help this
- TCP/IP stack ensures that application on host can only send/receive packets if application and IP address have equivalent SECLABEL
  - Support for servers or daemons that understand MLS (FTP, TELNET, INET)
    - Assign SYSMULTI SECLABEL to server/daemon
    - Can then communicate with any of the subnetworks

SECLABELs for z/OS UNIX Processes and Sockets

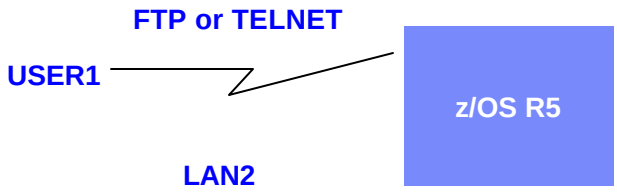
- Consider USER1 with access to
  - SECLABELs A and B
  - Workstations on three LANs
    - LAN1 defined with SECLABEL A
    - LAN2 defined with SECLABEL B
    - LAN3 defined with SECLABEL C

SECLABELs for z/OS UNIX Processes and Sockets



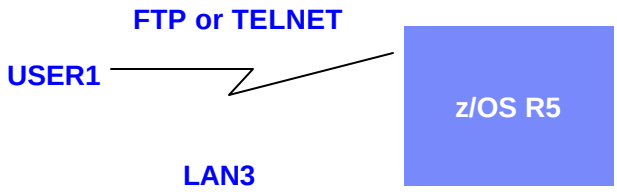
The user's session will run with SECLABEL A

SECLABELs for z/OS UNIX Processes and Sockets



The user's session will run with SECLABEL B

SECLABELs for z/OS UNIX Processes and Sockets



The user's session will fail, as he cannot use SECLABEL C

SECLABELs for z/OS UNIX Processes and Sockets

- Program access to SERVAUTH (enhancements to WHEN(PROGRAM) Conditional Access to the SERVAUTH class)
  - Allow appropriate use of PING and TRACEROUTE by a network administrator when multilevel security is enabled
    - Communications Server (TCP/IP) has the ability to restrict access to SERVAUTH resources to users running certain programs
- Allowed **ONLY** in a "**clean environment**" (like PADS – Program Access to Data Sets)
  - All programs previously loaded must be program-controlled
  - Uncontrolled programs cannot be loaded into the environment after access has been granted to the SERVAUTH based on the program name

To allow appropriate use of the "ping" and "traceroute" commands by a network administrator, when running with MLS functions enabled, Comm Server needs the ability to restrict access to SERVAUTH resources to users running certain programs. This can be done by allowing the specification of WHEN(PROGRAM(some_name)) for SERVAUTH general resource profiles.

To support this Comm Server requirement the PERMIT command has been changed to allow WHEN(PROGRAM) to be specified for the SERVAUTH class. Additionally, since Comm Server uses RACROUTE REQUEST=FASTAUTH rather than REQUEST=AUTH, WHEN(PROGRAM(...)) support has been added only to FASTAUTH processing. As with Program Access to Data Set, Program Access to SERVAUTH is only allowed in a clean environment; all programs previously loaded must be program-controlled, and no uncontrolled programs may be loaded into the environment after access is granted to the SERVAUTH based on the program name. Unlike Program Access to Data Set, PADCHK/NOPADCHK specification in the PROGRAM class has no meaning: only the current program's or first program's authority is checked.

SECLABELs for z/OS UNIX Files and Directories

- MAC protection for files and directories.
- RACF assigns user's SECLABEL to new file or directory when it is created.
  - SECLABEL cannot be changed.
    - Use the z/OS UNIX command, **chlabel**, to set one.
      - ★**R_setfsecl** - New callable service invoked by **chlabel** to set the SECLABEL of files or directories.
    - Copy the file to a directory with the appropriate SECLABEL to change it (subject to dominance and write-down).
  - Subdirectory has same SECLABEL as parent directory (except SYSMULTI).
  - Files in directory have same SECLABEL as directory.
- Enabled/Disabled via the new SETROPTS option **MLFSOBJ(ACTIVE / INACTIVE)**
  - Requires that UNIX Files and Directories have SECLABELs. It is similar to the existing option MLACTIVE.

- **R_setfsecl**
  - Users with **RACF SPECIAL** can set the SECLABEL of a file or directory if the FSP has a SECLABEL that is NOT blank or zero

SECLABELs for z/OS UNIX Files and Directories

- Root Directory:
  - SECLABEL determined at time data set containing the root directory is allocated.
  - Name of data set containing the root should have unique discrete profile or be covered by generic.
  - If file system is to contain data of multiple SECLABELs, the SECLABEL must be SYSMULTI.

The SECLABEL for the FSP of the root within each z/OS UNIX file system data set will be determined at the time the data set is allocated, via the standard data set SECLABEL association, and will be set by make_root_FSP when the SECLABEL class is active. The SECLABEL will either be an installation-defined SECLABEL or a special SECLABEL indicating that the file system may contain 'multilevel' contents. The special SECLABEL, SYSMULTI, will allow for file systems that contain data of multiple SECLABELs. **Note** The name of the data set containing the root should not match more than 1 discrete profile since the volume serial number is not available to make_root_FSP.

SECLABELs for z/OS UNIX Files and Directories

Since the zSeries file system (zFS) and the hierarchical file system (HFS) can both participate in shared sysplexes, note:

- The zSeries file system (zFS) supports security labels:
  - Symbolic links are protected by security labels.
  - Hard links are protected by security labels.
  - If a z/OS UNIX file, directory, or symbolic link was created in a zFS file system without being assigned a security label, the security administrator can assign a security label to it using the **chlabel** shell command (*).
- The hierarchical file system (HFS) does not fully support security labels.
  - If you want to use an HFS file system in read-write mode, and use security labels in the file system, you must copy or move it to a zFS file system.
  - The HFS file system does not support the name-hiding function.

- (*) That could happen for existing files and directories (created before enabling SECLABELs).
- For more information, see publication GA22-7509-00 - **Planning for Multilevel Security**

SECLABELs for z/OS UNIX Interprocess Communications

- MAC protection for
  - Pipes
  - UNIX Sockets
- Communication can only occur between processes with equivalent SECLABELs (a.k.a. EQUALMAC).
  - With limited exceptions:
    - The resource or the accessor SECLABEL is SYSMULTI.
- SECLABEL cannot be changed later.
- Enabled/Disabled via the new SETROPTS option **MLIPCOBJ(ACTIVE / INACTIVE)**
  - Requires that UNIX Interprocess Communications functions (shared memory, message queues, semaphores) have SECLABELs. It is similar to the existing option MLACTIVE.

- When creating an IPC security packet (ISP), if the SECLABEL class is active, RACF will copy the process SECLABEL, if one exists, into the ISP. Later, when checking access to the IPC for a subsequent connection, RACF will reject the request if the current process does not have a SECLABEL or the SECLABEL does not match. Once a SECLABEL has been assigned to an IPC object, there is no way to change it.
- Access checking for IPC objects will be treated as EQUALMAC checking, meaning that SECLABELs must be equivalent, unless the resource's SECLABEL is SYSMULTI, or the accessor's SECLABEL is SYSMULTI. While most classes require the specification of EQUALMAC=YES in the class descriptor table IPC access checking will not rely on this.

SECLABEL By System

- Allows customer to 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, e.g.
  - SYSHIGH, SYSLOW, SYSNONE, SYSMULTI
- Enabled/Disabled via the new SETROPTS option **SECLBYSYS/NOSECLBYSYS**

In a SYSPLEX where many SYSPLEX members share the same RACF database, the ability to limit the use of SECLABELs to certain members may be a desirable function. This allows one member of the SYSPLEX to run work at SECLABEL A, while another handles SECLABEL B, keeping work separated based on security classification, while still sharing the RACF database. The specification of ADDMEM(SYSID) to the SECLABEL definition will allow SECLABELs to be activated on a per-system basis. Activation occurs when a SETR RACLIST(SECLABEL) REFRESH is issued after activating a new SETR option, SECLBYSYSTEM. To ensure jobs are submitted and execute on systems with the correct SECLABEL, JES will determine which SECLABELs are active on each system.

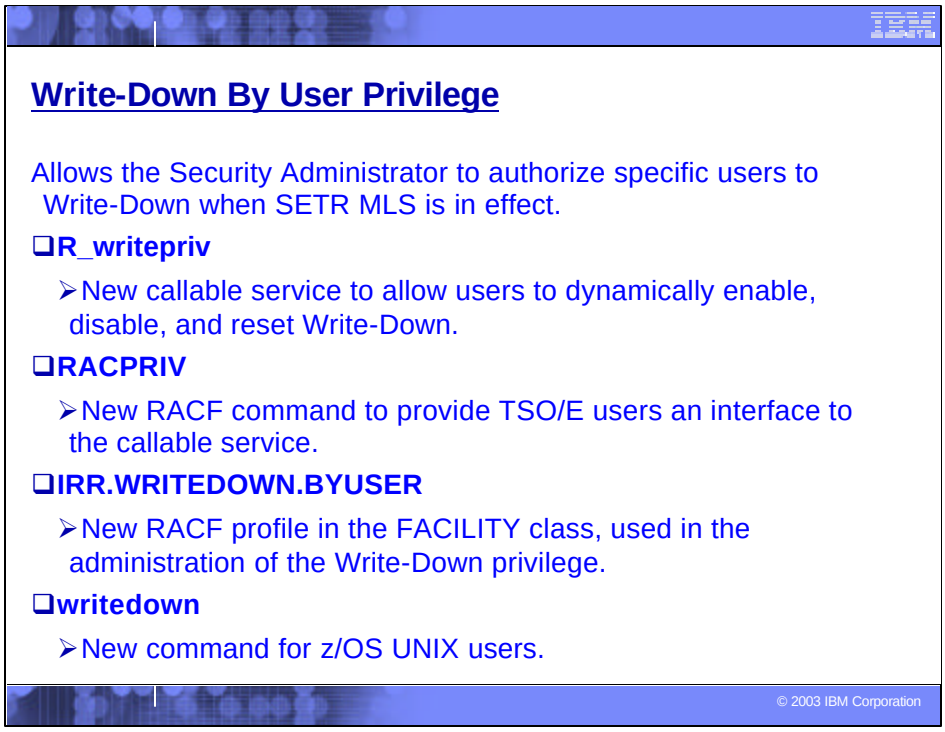
SECLABEL By System

- Example:
  - SECLABELs A, B, and C
  - 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.

- RLIST, LISTDSD, SEARCH
  - List ONLY those profiles that have Active SECLABELs

SECLABEL By System

- New operand SIGNAL= added on the ICHERCDE macro
- Enhancements to SETROPTS processing for SECLABEL By System:
  - New ENF Signal is sent to listeners for those CDT classes that have SIGNAL=YES for
    - SETR RACLIST
    - SETR RACLIST REFRESH
    - SETR NORACLIST
- For the SECLABEL class, allows JES to keep a current list of active SECLABELs by listening for this signal.



- Write-Down privilege can be assigned to individual users that allows them to select the ability to write-down when SETR MLS is in effect. Users who have been assigned this privilege can enable and disable their ability to write-down.
- The write-down by user privilege can be activated and deactivated on a system through the creation of the FACILITY class profile IRR.WRITEDOWN.BYUSER.
  - Users with READ access can request Write-Down privilege
  - Users with UPDATE access can request Write-Down privilege and have it by default
- It is only checked if SETR MLS(FAILURES) or SETR MLS(WARNING) has been activated.
- Authority checking has been modified in RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE.
- VERIFY/VERIFYX has also been modified.
  - A bit in the UTOKEN is set to indicate whether or not the user has the write-down privilege enabled. When the UTOKEN is built, the write-down privilege will be indicated if the user has it enabled by default.
- The new callable service, IRRSWP00, will allow users who have the write-down privilege to enable it, disable it, or reset it to the default setting, resulting in the resetting of the UTOKEN indicator. They can also query the current setting. The callable service provides the auditing.

Name Hiding

Allows installations to prevent users from discovering data set names, file names, and directory names that they didn't already know.

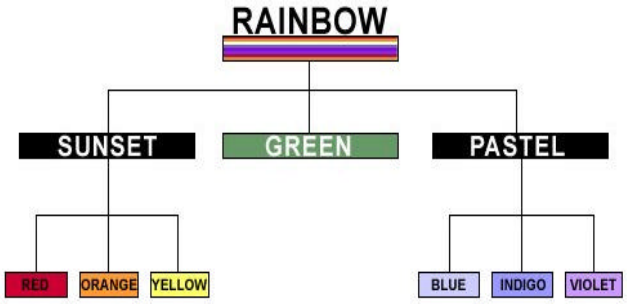
- Enabled/Disabled via the new SETROPTS option **MLNAMES/NOMLNAMES**
- Needed only if
  - The dataset names contain sensitive data
  - The file names contain sensitive data
- Should not be enabled, unless necessary, because it can cause performance degradation.

- Currently:
  - Users with the ability to list the VTOC of a volume or list the entries in a catalog can see the names of many data sets.
  - z/OS UNIX users issuing the **ls** command against a SYSMULTI directory can see the names of subdirectories and files with differing security.
- This new function will prevent these from happening.
- Note that SECLABELs are not required to use some parts of this support. Data set names will be hidden if a user does not have at least read access to a DATASET profile based on discretionary access checking. For files and directories, however, this option results only in a check of security labels, which will always be considered successful if the SECLABEL class is inactive.

Miscellaneous Enhancements

- **SECLABEL support for FASTAUTH**
  - FASTAUTH was modified to provide support for SECLABELs
- Auditing
  - Two new Event Codes.
  - New Event Code Qualifiers and Relocate sections added to a number of events.
- **Enhancements to RACF Utilities**
  - In addition to the changes in UT200 and DB Unload for SERVAUTH, the following utilities have been enhanced:
    - SMF Unload
    - SAF Trace

SECLABEL Hierarchy



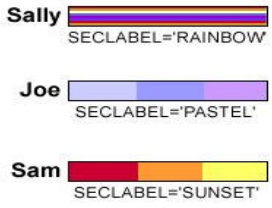
With the hierarchy established in the security manager layer, the system would understand that users with authority to read RAINBOW can read anything. Someone with authority to read PASTEL information can read any row associated with BLUE, INDIGO, VIOLET, or PASTEL. Someone with SUNSET can read SUNSET, RED, ORANGE, YELLOW. This is a lot more powerful than just having an exact match on SECLABEL (i.e., user's label must exactly match the data's label), since it has the notion of "groups" (in this case, sets of categories) that make security administration easier to manage.

With this additional capability, DB2 is able to implement that type of security scheme without requiring the application to access the data using special views or predicates.

See
http://www7b.boulder.ibm.com/dmdd/library/techarticle/0209cotner/0209cotner.html

Multilevel Security and DB2

Row Granularity Multilevel Security



DB2_SECURITY_LABEL_EXT	COL1	COL2	COL2
RAINBOW	56	7	76
RAINBOW	24	56	65
RAINBOW	42	6	45
BLUE	3	456	7
INDIGO	113	456	56
VIOLET	3	456	4
BLUE	4	4556	7
RED	4	76	567
ORANGE	33	7	567
RED	5455	76	567
YELLOW	999	65	45

- ❑Table column defined AS SECURITY LABEL
- ❑Check for each new SECLABEL value accessed
- ❑Mandatory access control: run time user to data

Row-level security for applications that need more granular security or mandatory access control. For example, an organization may want a hierarchy in which employees can see their own payroll data, a first line manager can see his or her payroll information and all of the employees reporting to that manager, and so on. Security schemes often include a security hierarchy and non-hierarchical categories. You can add a column that acts as the security label (SECLABEL) with a column defined AS SECURITY LABEL: Each row value has a specific SECLABEL. The SECLABELs are defined and provided by RACF for a user, then saved in rows for INSERT, UPDATE, LOAD, …

When rows are accessed, DB2 checks for each new SECLABEL value accessed. If access is allowed, then, normal access. If access is not allowed, data is not returned. This is runtime user SECLABEL to data checking, in addition to grant and permit controls.

Multilevel Security and DB2

Multilevel Security with Row Level Granularity

- Use RACF for MAC
  - Use SECLABELs
  - Key advantage is consistent, integrated security
- Table has a column defined as a security label
  - Each row value has a specific security label
  - Get user security label from RACF
  - Save in rows for INSERT, UPDATE, LOAD, ...
- Compare SECLABEL in row to SECLABEL for the DB2 users
  - If access is allowed, then normal access
  - If access is not allowed, data not returned
- Runtime user to data checking
- Seclabel values are cached to minimize processing time

Multilevel Security and DB2

CREATE TABLE / ALTER TABLE statements

- Use To enable the row level security
  - Table must have a column to store the SECLABEL
- To define the security label column
  - Specify "**AS SECURITY LABEL**" in the column-options in the "**create table / alter table**" column-definition
- Table once created with SECLABEL cannot be disabled
- Audit record produced if the table with security label is created, altered or dropped

When you CREATE a table or ALTER it, you can decide to implement row-level security by including or adding a column that is specified AS SECURITY LABEL. The column must be defined as CHAR(8).

The only technique to disable this security is to drop the table, table space or database.
Any column name can be the security label, but the same column name cannot be used more than once in the a table. Only one security label is allowed in a table.

The security label column must be data type single byte character, char(8), NOT NULL WITH DEFAULT. This column cannot have field procedures, edit procedures or check constraints.

Multilevel Security and DB2

Using SECLABELs with Row operations:

- **SELECT**
  - User's SECLABEL compared to SECLABEL of row
    - If user SECLABEL dominates the data SECLABEL
      - Row is returned
    - If user SECLABEL does not dominate the data SECLABEL
      - Row is not returned, but no error is reported

Multilevel Security and DB2

Using SECLABELs with Row operations:

- **INSERT**
  - Value of the SECLABEL column for inserted row is set to the value of the user's SECLABEL.
    - If user has authority for Write-Down, then the user is allowed to set the SECLABEL field to any value.
    - If user does not have authority for Write-Down, then the SECLABEL of the inserted rows will be set to current SECLABEL.

Multilevel Security and DB2

Using SECLABELs with Row operations:

- **UPDATE**
  - User's SECLABEL compared with the SECLABEL of the row to be updated.
    - If the SECLABELs are equivalent
      - Row is updated.
      - The SECLABEL in updated row is set to the user SECLABEL.
    - If user has Write-Down authority, then rows with lower SECLABELs can be accessed and updated.

Multilevel Security and DB2

Using SECLABELs with Row operations:

- **DELETE**
  - User's SECLABEL compared with the SECLABEL of the row to be deleted.
    - If the SECLABELs are equivalent
      - Row is deleted.
    - If user has Write-Down authority, then rows with lower SECLABELs can be accessed and deleted.

References

- Security Server (RACF) publications:
  - RACF Command Language Reference (SC28-1919)
  - RACF Security Administrator's Guide (SC28-1915)
  - RACF Callable Services Guide (SC28-1921)
- z/OS publications:
  - Planning for Multilevel Security (GA22-7509-00)
- RACF web site:
  http://www.ibm.com/servers/eserver/zseries/zos/racf
- DB2 web site:
  http://www.ibm.com/software/db2zos
  - Related publications / presentations:
    http://www.ibm.com/software/db2zos/db2zosv8.html
    http://www.ibm.com/software/db2zos/presentations.html
    http://www.ibm.com/software/db2zos/support.html

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - CICS
  - DB2
  - MVS
  - MVS/ESA
  - OS/390
  - RACF
  - S/390
  - z/OS
- UNIX is a registered trademark of The Open Group in the United States and other countries.