



Session RAB7

Intro to z/OS Multilevel Security (MLS)

Walt Farrell, CISSP, z/OS Security Design, IBM

Vanguard Security Expo
June, 2007

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2*
e-business logo
IBM*
IBM eServer
IBM logo*
OS/390*
RACF*
z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Table of Contents

- Why Multilevel Security?
- What is Multilevel Security?
- Commercial Exploitation
- General SECLABEL Considerations and Options
- Multilevel Security with TCP/IP
- Multilevel Security with JES
- Multilevel Security with DB2
- References
- Trademarks

Why Multilevel Security?

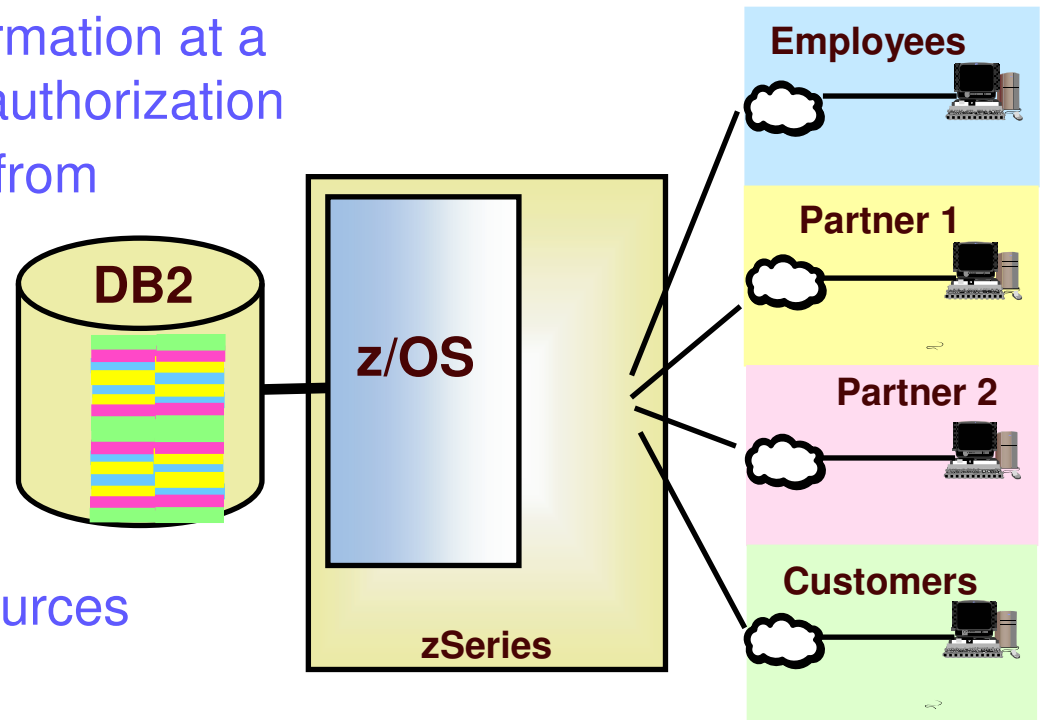
- ❑ Highly secure data
- ❑ Shared between people/organizations with different "need to know".
 - Multilevel Security provides a way to segregate users and their data from other users and their data regardless of access lists, UACC, etc.
- ❑ Must be
 - Manageable, Affordable, Resilient, Highly available
- ❑ Valuable to government agencies
 - Use of functions like name-hiding, write-down, *-property (no write-down)
- ❑ Valuable to commercial clients (e.g. service bureau)
 - Can be set up using a small set of SECLABELs and a few SETROPTS options (MLACTIVE and SECLABELCONTROL)
 - Most SECLABEL-related SETROPTS options not needed for commercial use

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

What is Multilevel Security?

- ❑ A secure computing environment with two goals:
 - Controls to prevent unauthorized individuals from accessing information at a higher classification than their authorization
 - Controls to prevent individuals from declassifying information
- ❑ Controls
 - Classifies data using
 - Security Levels
 - Security categories
 - System controls access to resources
 - Labels all resources
 - Enforces accountability
 - Prevents 'declassifying' data
 - Does not allow reuse of data objects until purged



**Multilevel Security
on zSeries**

Commercial Exploitation

- ❑ Application servers shared across multiple customer constituencies
 - Labeling allows data to be compartmentalized or isolated from other customers
 - ❖ Data protected for competitive, privacy and integrity reasons
 - Labeling of data and application identities provides the means for both the aggregation and compartmentalization of data.

- ❑ zSeries is able to host large databases on behalf of transaction programs or other application servers
 - Facilitates some database aggregation that reduces execution costs

- ❑ Database on demand capability
 - Functionality is provided by strength of security on z/OS and within DB2
 - DB2 z/OS V8 row-level security and z/OS V1R5 with RACF provide the operating system and security services that make database on demand capability whole

Application serving on demand

- ❑ Service business acquires a collection of servers and hosts a specific application and its associated data on that server infrastructure.
- ❑ Sells subscriptions for the application to other businesses
 - Subscribers need their data isolated from other businesses
- ❑ Make a subset of the information available by aggregating data using labels. Isolate sensitive data.
- ❑ Saves server and network costs associated with replicating data across business units.

Outsourcer running an application practice

Common DB schema across customers

Seclabel="customer_name"

DB2_SECURITY_LABEL_EXT	COL1	COL2	COL3
Customer A			
Customer B			
Customer A			
Customer B			
Customer C			
Customer D			
Customer E			
Customer A			
Customer B			
Customer D			
Customer E			

Figure 2 - Using security labels for application serving on demand

Financial services on demand

- ❑ Government regulations may inhibit one business unit from seeing personal consumer information associated with another business unit.
- ❑ Subset of information may be valuable for data mining
 - Identifying trends
 - Developing new services
- ❑ Make a subset of the information available by aggregating data using labels. Isolate sensitive data.
- ❑ Saves server and network costs associated with replicating data across business units.

Large company managing HR for subsidiaries
 "corporate phone book"
 Seclabel="subsidiary_name"

DB2_SECURITY_LABEL_EXT	COL1	COL2	COL3
Subsidiary 1			
Subsidiary 2			
Subsidiary 3			
Subsidiary 1			
Subsidiary 4			
Subsidiary 2			
Subsidiary 3			
Subsidiary 4			
Subsidiary 1			
Subsidiary 2			
Subsidiary 4			

Figure 3 - Using security labels for financial services on demand

Commercial on demand services summary

- ❑ Security labeling of data and application identities
 - Provides both compartmentalization and aggregation of data

- ❑ Need to replicate or move data to provide a new security container or isolation point?
 - Consider labeling
 - ✓ Save on processor, network, storage and administrative expense

- ❑ Examine database organization and flow of data between application servers
 - Labeling may provide additional security and deployment savings to your business

Original SECLABEL support (before z/OS V1R5)

- ❑ RACF and other evaluated system components support Security Labels (aka SECLABELS).

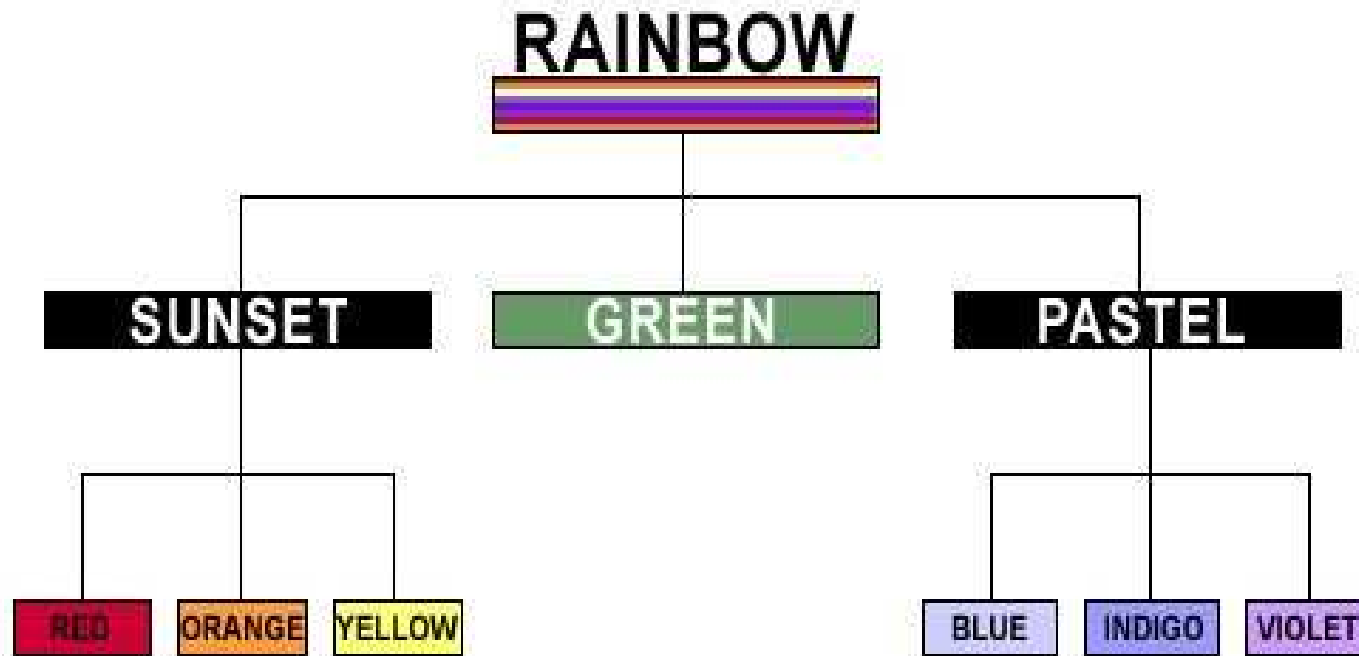
- ❑ SECLABELS have two components:
 - Level (a named number in the range 1-254)
 - Unclassified/1
 - Sensitive/25
 - Confidential/50
 - Secret/100
 - List of Categories (0 or more named categories)
 - Green
 - Yellow, Orange
 - Yellow, Orange, Red

- ❑ For commercial usage, the categories are probably more important than the level, and most SECLABELS may use the same level, but different sets of categories.

SECLABEL Dominance

- ❑ SECLABELs defined
 - **RED**
 - SECLEVEL = SECRET
 - CATEGORY = PROJA, PROJ B, PROJ C, PROJ D, PROJ E
 - **ORANGE**
 - SECLEVEL = SENSITIVE
 - CATEGORY = PROJA, PROJ B, PROJ C, PROJ E
 - **GREEN**
 - SECLEVEL = SENSITIVE
 - CATEGORY = PROJ C, PROJ D, PROJ E
 - **BLUE**
 - SECLEVEL = UNCLASSIFIED
 - CATEGORY = PROJ E
- ❑ **RED** dominates all
- ❑ **ORANGE** & **GREEN** dominate BLUE
- ❑ **ORANGE** & **GREEN** are disjoint security labels

SECLABEL Hierarchy



Session SECLABEL Assignment

- ❑ Each user has a default SECLABEL
- ❑ A user may have access to other SECLABELs, too
- ❑ Some applications (TSO/E, batch jobs) support user requesting a specific SECLABEL
- ❑ Each port of entry (TERMINAL, TCP/IP security zone, ...) has a SECLABEL
- ❑ Each SECLABEL has a RACF profile
 - Access list
 - Universal access
 - Auditing
- ❑ During user authentication, depending on application, user may request a SECLABEL, or RACF may infer one from the port of entry or application, or assign the user's default
- ❑ RACF validates session SECLABEL
 - User must have access to that SECLABEL
 - SECLABEL must properly match the port of entry and application

Some SECLABEL-related Options

- ❑ MACTIVE – Requires users and some resources to have SECLABELs
- ❑ SECLABELCONTROL – Restricts who can assign SECLABELs to resources
- ❑ SECLABELAUDIT – Allows audit generation based on user SECLABEL or (new in z/OS R6) resource SECLABEL
 - Good for logging access to especially restricted data (privacy, financial)
- ❑ Possibly MLS – Prevents “write down” (prevents, for example, a user running with SUNSET from writing to a file or data set with the RED SECLABEL.
- ❑ If using SETROPTS MLS, then you can also allow selected users to “write down” in a controlled fashion, via the RACPRIV command.

Resource Access Checking & SECLABELs (Commercial Use)

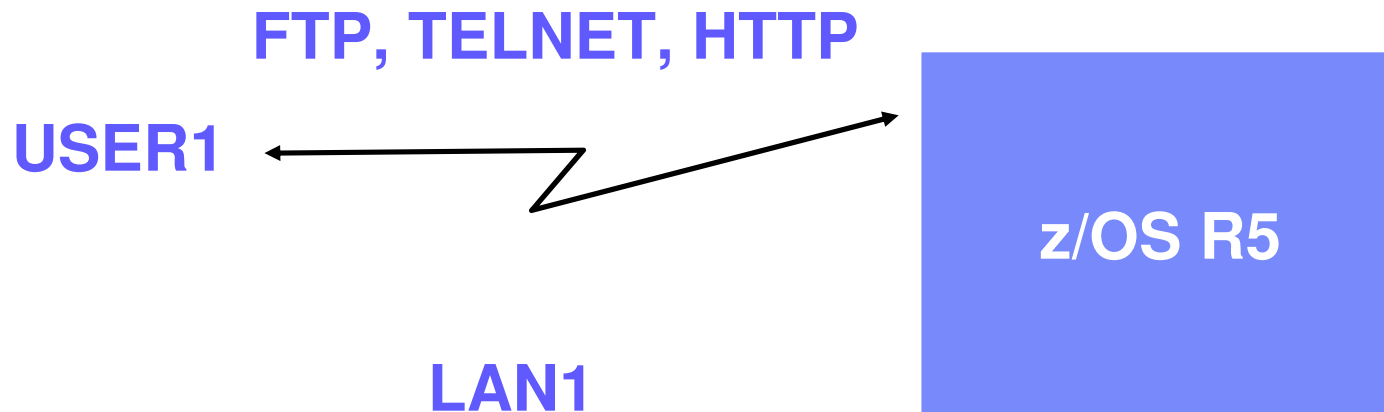
- ❑ User tries to access resource
 - RACF compares user's SECLABEL and resource's SECLABEL
 - Reading: User SECLABEL > resource SECLABEL
 - Updating: (without SETROPTS MLS, or if user has WRITEDOWN authority)
 - User SECLABEL > resource SECLABEL or
 - Resource SECLABEL > User SECLABEL
 - Updating: (with SETROPTS MLS)
 - User SECLABEL = resource SECLABEL

SECLABELs for TCP/IP

- ❑ Administrator can define “security zones” representing IP subnetworks via TCP/IP configuration data
 - Specifies hostname, or address, or subnet range
 - Any granularity desired, down to individual IP address if needed
 - Specifies a “zone” name. Example: INTERNAL, EXTERNAL, PARTNER1
- ❑ TCP/IP maps zone names to RACF SERVAUTH resource EZB.NETACCESS.sysname.stackname.zonename
 - Installation is 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 appropriate SECLABELs
 - Support for servers or daemons that understand MLS (FTP, TELNET, INET) or even HTTP for some usage
 - Assign SYSMULTI SECLABEL to server/daemon
 - Can then communicate with any of the subnetworks

SECLABELs for TCP/IP

- 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



The user's session will run with SECLABEL A

SECLABELs for TCP/IP

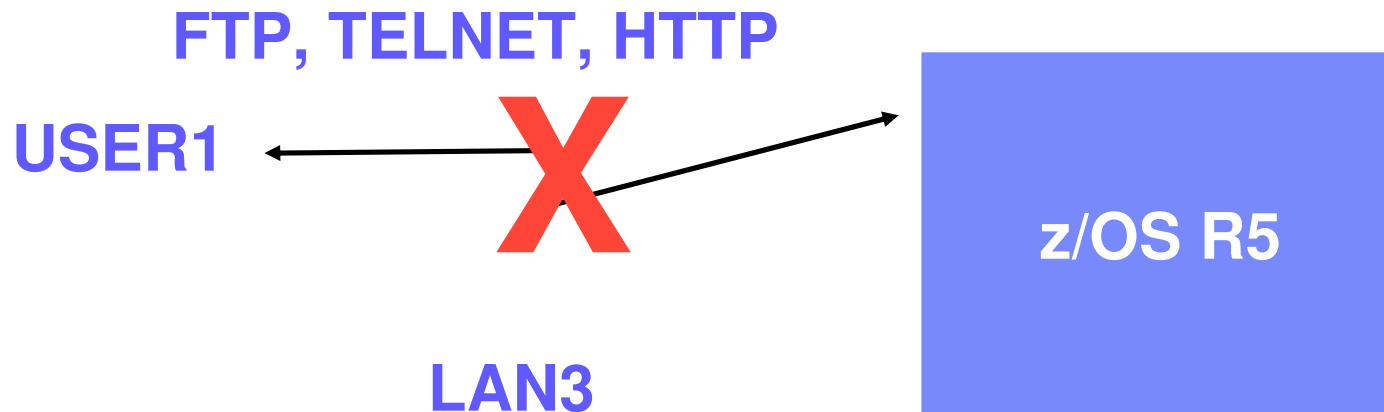
- ❑ Consider USER1 with access to
 - SECLABELs A and B
 - Workstations on three LANs
 - LAN1 defined with SECLABEL A
 - LAN2 defined with SECLABEL B
 - LAN3 defined with SECLABEL C



The user's session will run with SECLABEL B

SECLABELs for TCP/IP

- ❑ 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



**The user's session will fail,
since the user cannot use SECLABEL C**

Multilevel Security with JES

- Consider a Service Bureau with multiple customers
- Customer A does not want their output printed on Customer B's printers
- Create disjoint SECLABELs A and B
- Create WRITER profiles for customer A printers; assign SECLABEL A
- Create WRITER profiles for customer B printers; assign SECLABEL B
- Customer A users (with SECLABEL A) cannot print to wrong printers
- Customer B users (with SECLABEL B) cannot print to wrong printers
- System operators cannot misdirect the output, either

Multilevel Security on z/OS V1R5 and DB2 V8

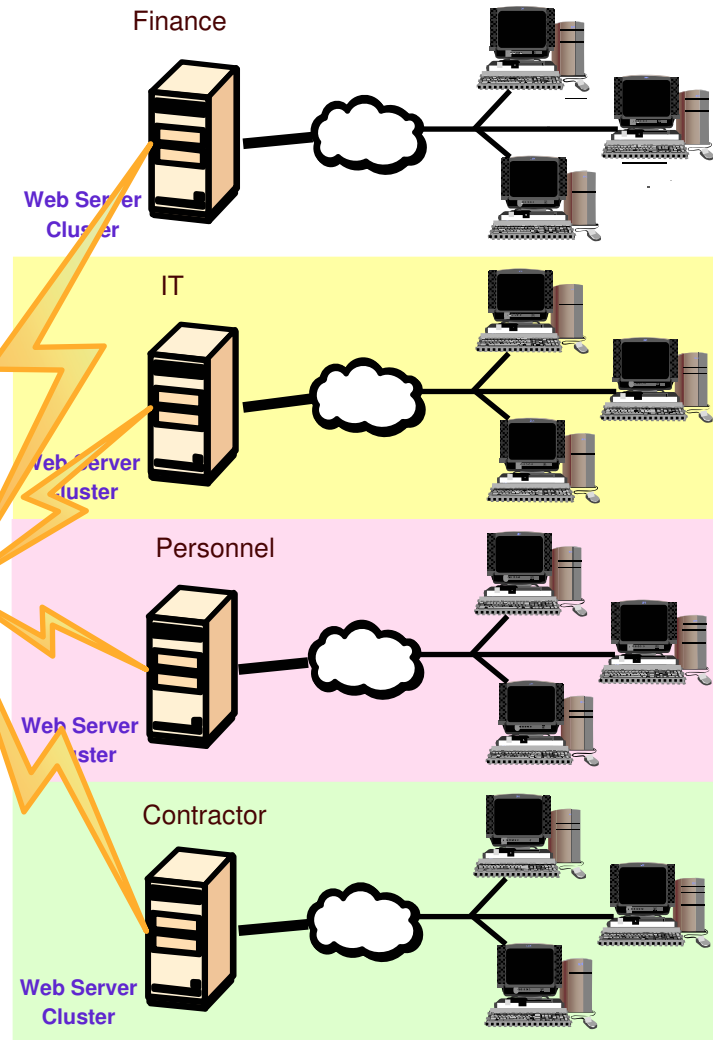
- ❑ Multilevel Security on z/OS V1R5 with DB2 V8
 - Labeled security allows sharing of resources with mixed levels of security in a single image
 - Example: Single image of data sharable by multiple enterprise departments with different need to know

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
Personnel	22	Germany	9%
IT	87	USA	14%
Contractor	23	UK	20%
Personnel	34	Germany	43%
Finance	981	USA	12%
IT	223	USA	10%
Contractor	45	Canada	29%

Data

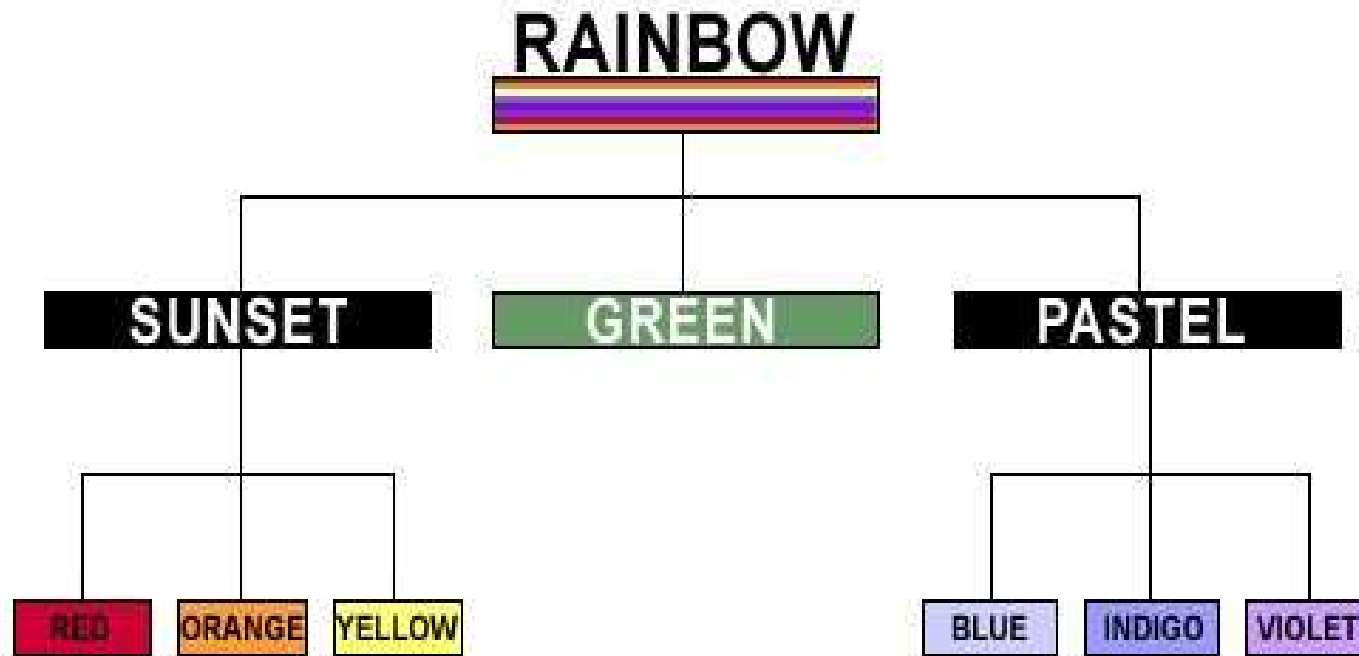
Single Data Store

DBMS Server



Multilevel Security on zSeries


SECLABEL Hierarchy



Multilevel Security and DB2

Row Granularity Multilevel Security

Sally 
SECLABEL='RAINBOW'

Joe 
SECLABEL='PASTEL'

Sam 
SECLABEL='SUNSET'

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

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

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,
 - The user is allowed to set the SECLABEL field to any valid value.
 - If user does not have authority for Write-Down,
 - 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,
 - 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,
 - 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)
- ❑ Communications Server Publications:
 - IP Configuration Guide (SC31-8775)
 - IP Configuration Reference (SC31-8776)
- ❑ 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>