

# Multilevel Security – What's New?

## Vanguard Enterprise Security Expo

June, 2004

Walt Farrell

z/OS Security Server Design

Telephone: (845) 435-7750

e-mail: [wfarrell@us.ibm.com](mailto:wfarrell@us.ibm.com)



# Table of Contents

- ❑ Why Multilevel Security?
- ❑ What is Multilevel Security?
- ❑ What is the problem?
- ❑ The solution - Multilevel Security on zSeries
- ❑ History & Evolution
- ❑ Existing B1 Support (before z/OS V1R5)
- ❑ z/OS V1R5 Multilevel Security Enhancements
  - SECLABELs and MAC checking
  - 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
  - Write-Down by User privilege
  - Name Hiding
  - Miscellaneous Enhancements
- ❑ Multilevel Security on z/OS V1R5 and DB2 V8
- ❑ References
- ❑ Trademarks

## Why Multilevel Security?

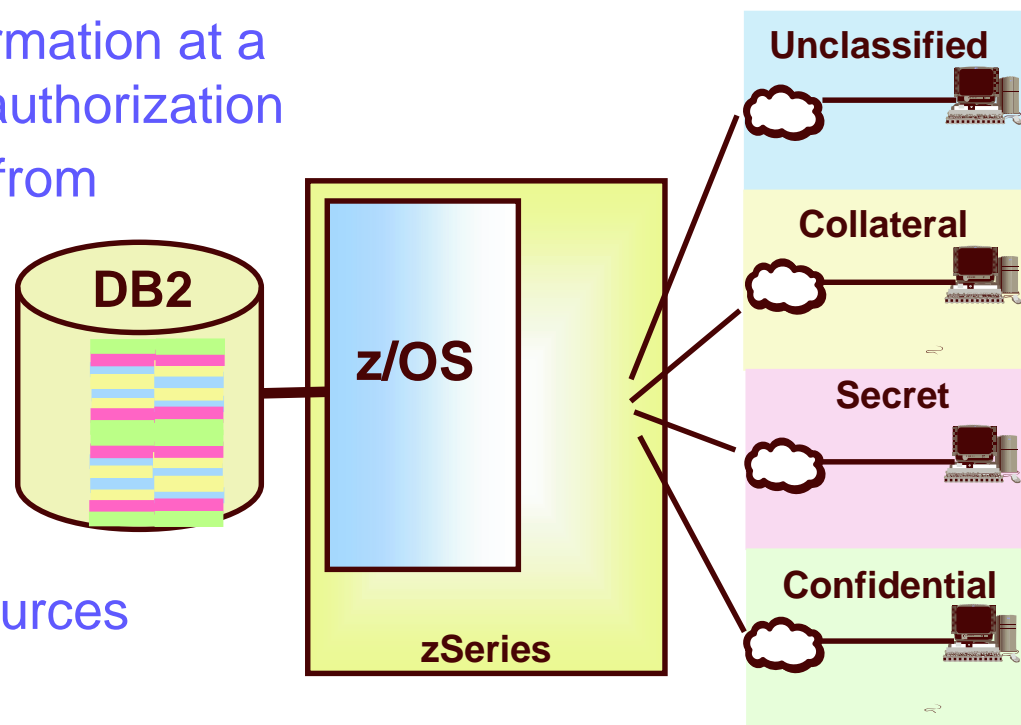
- ❑ Highly secure data
- ❑ Shared between people/organizations with different "need to know".
  - Multilevel Security provides a way to segregate users and their data from other users and their data regardless of access lists, UACC, etc.
- ❑ Must be
  - Manageable, Affordable, Resilient, Highly available
- ❑ Valuable to government agencies
  - Use of functions like name-hiding, write-down, \*-property (no write-down)
- ❑ Valuable to commercial clients (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

# 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

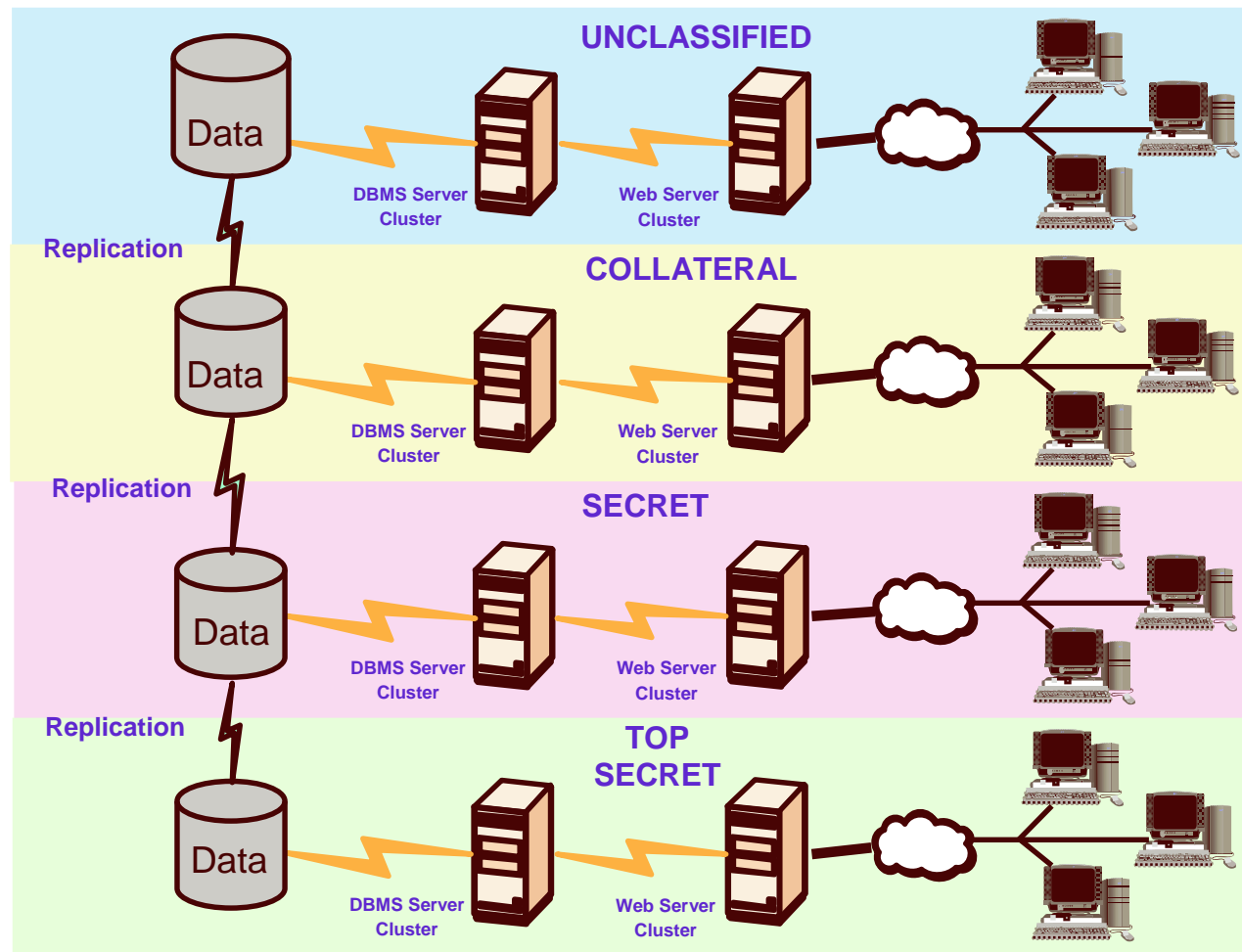


**Multilevel Security  
on zSeries**

# What is the problem?

- ❖ Separate servers required for each security compartment
- ❖ Data is replicated between database servers
- ❖ Costly to implement and manage
- ❖ Infrastructure could be multiplied many times for each application or managing organization

## Without Multilevel Security



# The solution! - Multilevel Security on zSeries

## □ Proven mainframe reliability and quality of service

### ➤ Self-optimizing

- Managing to business priorities:  
z/OS Workload Manager
- Managing resources:  
Intelligent Resource Director
- Managing storage: z/OS DFSMS

### ➤ Robust z/OS security:

- RACF & PKI Services
- Intrusion Detection Services
- Address Space Isolation

### ➤ zSeries cryptography

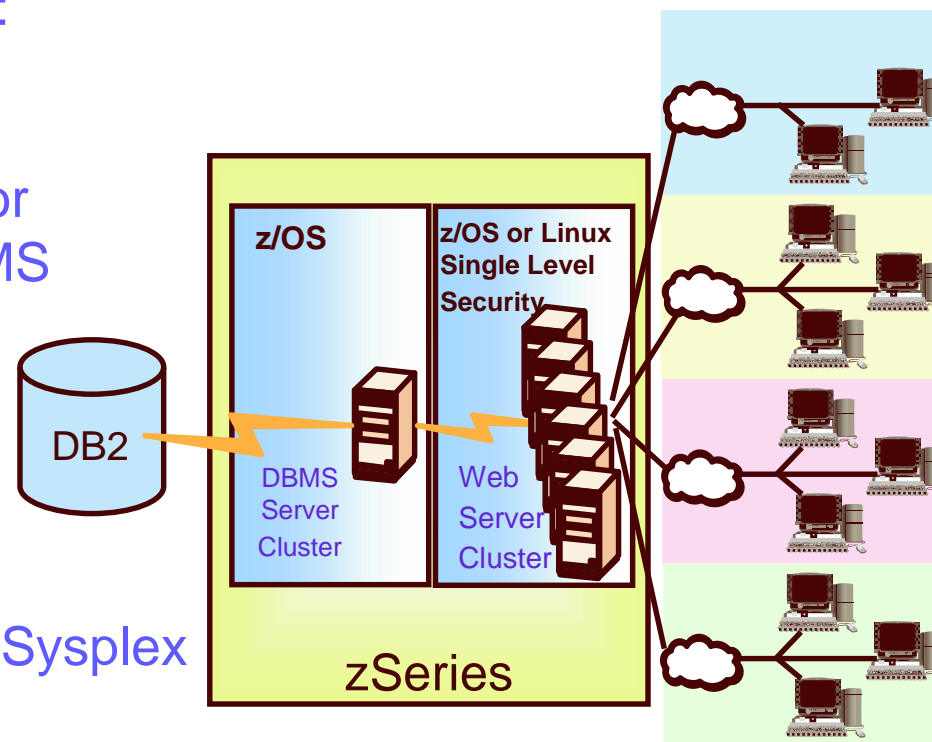
### ➤ Scale and high availability: Parallel Sysplex

### ➤ Business recovery: GDPS

(Globally Dispersed Parallel Sysplex)

### ➤ Server consolidation:

- Linux for zSeries or z/OS for Web Serving
- Secure Partitions: LPARS certified at Common Criteria EAL5



**Multilevel Security  
on zSeries**

## Multilevel Security for zSeries

- ❑ Designed, developed, and tested to meet the requirements of the Common Criteria
  - MAC/DAC support using labeled resources
  
- ❑ "COTS" - Commercial Off-the-Shelf products
  - DB2 with z/OS
  
- ❑ Certification planned
  - IBM announcement made on February 12th, 2004:
    - ❖ “z/OS 1.6 is currently in evaluation for Common Criteria certification to the Labeled Security Protection Profile (LSPP) at EAL3+. Evaluation for certification for Controlled Access Protection Profile (CAPP) to the EAL3+ is also in progress.”

# 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, Communications Server (TCP/IP), “not designed for B1”.
- ❑ Common Criteria Developed
  - Internationally recognized standard ISO15408
  - US National Security Agency sponsored
  - Defined functional and assurance (process) requirements
- ❑ US intelligence community driving requirements to meet Common Criteria
- ❑ ~2004
  - With z/OS V1R5 IBM extends “B1” support to cover these functions.



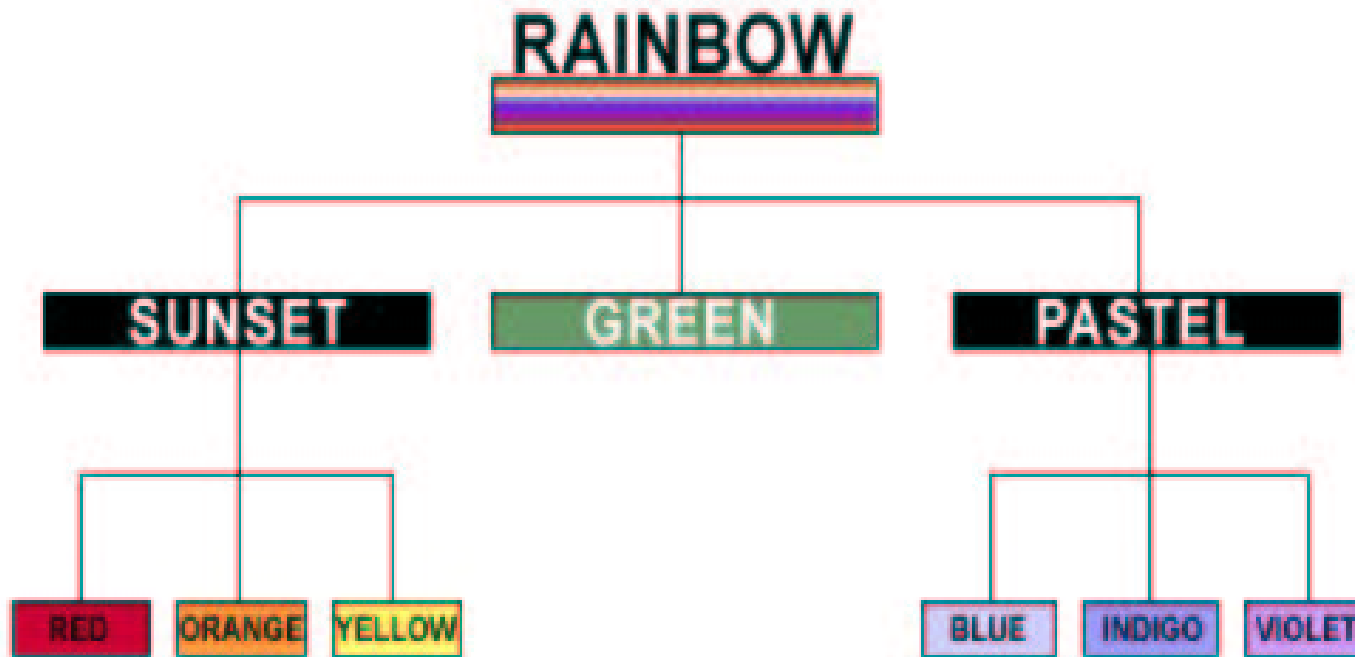
## Existing B1 support (before z/OS V1R5)

- ❑ 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

## 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

# SECLABEL Hierarchy



## 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
- ❑ 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

## 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

## z/OS V1R5 Multilevel Security enhancements

### □ New special system-defined SECLABEL

#### ❖ **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



## SECLABELs for z/OS UNIX Processes and Sockets

- ❑ Prior to z/OS V1R5, 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.

## SECLABELs for z/OS UNIX Processes and Sockets

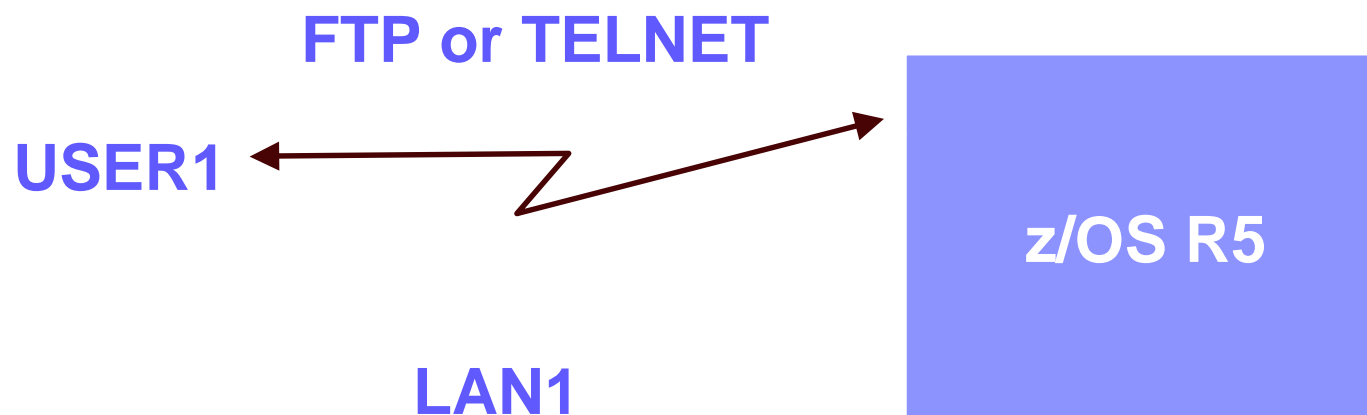
- ❑ SERVAUTH class usage and characteristics have been enhanced to accommodate IP V6 addresses.
- ❑ New parameters have been added to InitACEE to allow the SECLABEL and SERVAUTH values to be passed.
- ❑ Corresponding changes have been made to allow applications to pass these values through UNIX System 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

## 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
  - 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 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

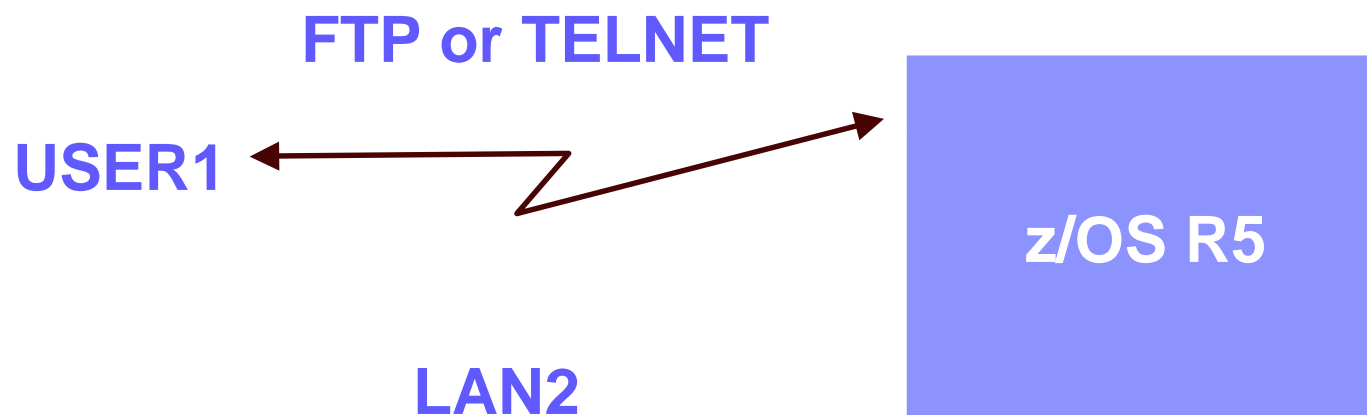
- ❑ Consider USER1 with access to
  - SECLABELs A and B
  - Workstations on three LANs
    - LAN1 defined with SECLABEL A
    - LAN2 defined with SECLABEL B
    - LAN3 defined with SECLABEL C



The user's session will run with SECLABEL A

## SECLABELs for z/OS UNIX Processes and Sockets

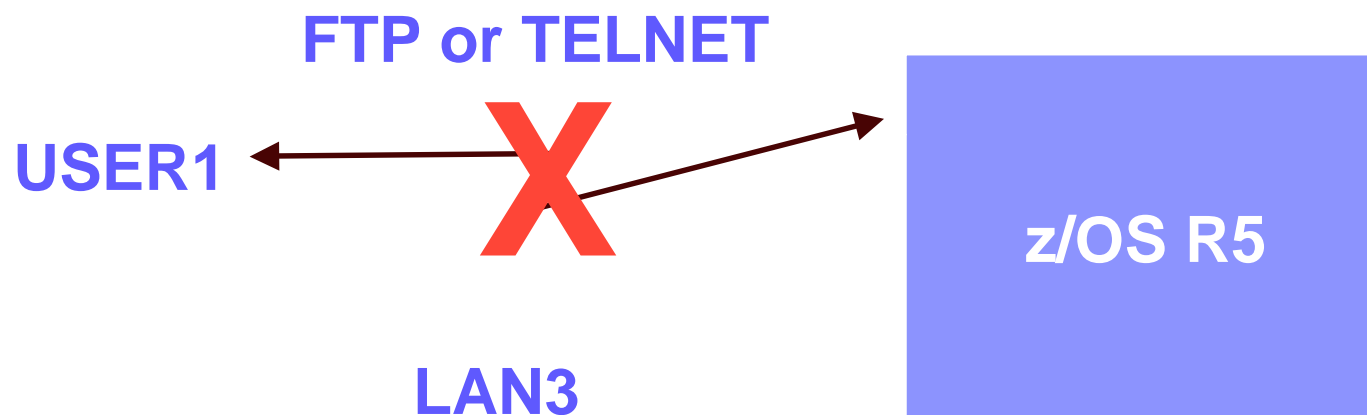
- ❑ Consider USER1 with access to
  - SECLABELs A and B
  - Workstations on three LANs
    - LAN1 defined with SECLABEL A
    - LAN2 defined with SECLABEL B
    - LAN3 defined with SECLABEL C



The user's session will run with SECLABEL B

## 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



The user's session will fail,  
since the user 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

## SECLABELs for z/OS UNIX Files and Directories

- ❑ MAC protection for files and directories.
- ❑ RACF assigns a SECLABEL to new file or directory when it is created.
  - 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.
  - Subdirectory has same SECLABEL as parent directory (except SYSMULTI).
  - Files in directory have same SECLABEL as directory (except SYSMULTI).
- ❑ Enabled/Disabled by activating the SECLABEL class
- ❑ Enforced via the new SETROPTS option

### **MLFSOBJ(ACTIVE / INACTIVE)**

- Requires that UNIX Files and Directories have SECLABELs. It is similar to the existing option MACTIVE.



## SECLABELs for z/OS UNIX Files and Directories

- ❑ 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).

## 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.

## SECLABELs for z/OS UNIX Interprocess Communications

- ❑ MAC protection for
  - IPC Objects (shared memory, message queues, semaphores)
  - Sigqueue
  - Pipes
  - UNIX Sockets
  - PTrace
- ❑ 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 by activating the SECLABEL class
- ❑ Enforced via the new SETROPTS option **MLIPCOBJ(ACTIVE / INACTIVE)**
  - Requires that UNIX IPC Objects have SECLABELs. It is similar to the existing option MLACTIVE.

## 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**

## 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.

## 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 By User Privilege

Allows the Security Administrator to authorize specific users to Write-Down when SETR MLS is in effect.

### ❑ **R\_writepriv**

- New callable service to allow users to dynamically enable, disable, and reset Write-Down.

### ❑ **RACPRIV**

- New RACF command to provide TSO/E users an interface to the callable service.

### ❑ **IRR.WRITEDOWN.BYUSER**

- New RACF profile in the FACILITY class, used in the administration of the Write-Down privilege.

### ❑ **writedown**

- New command for z/OS UNIX users.

## 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.



## 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.

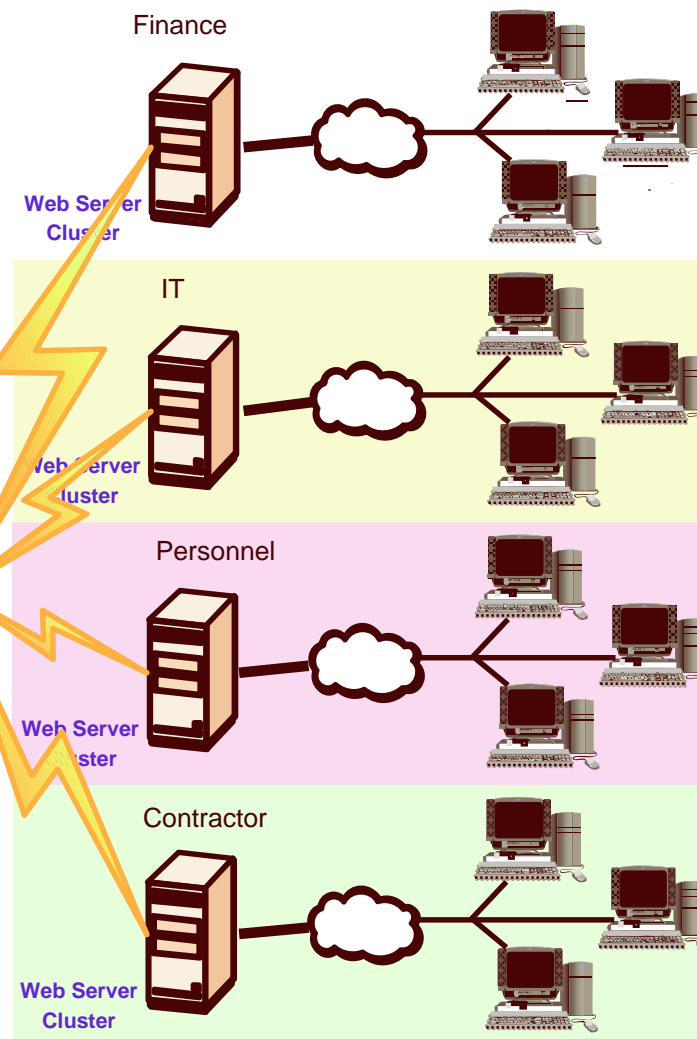
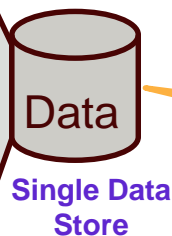
### ❑ **Enhancements to RACF Utilities**

- In addition to the changes in UT200 and DB Unload for SERVAUTH, the following utilities have been enhanced:
  - SMF Unload
  - SAF Trace

# Multilevel Security on z/OS V1R5 and DB2 V8

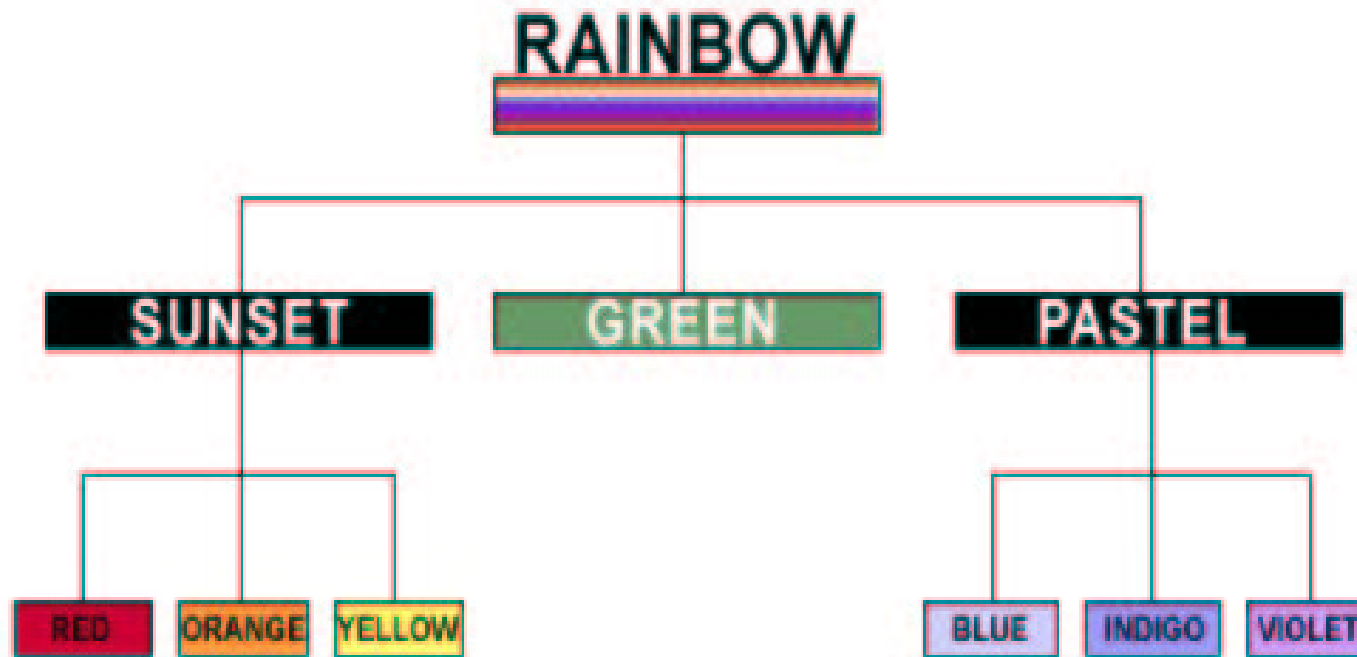
- ❑ Multilevel Security on z/OS V1R5 with DB2 V8
  - Labeled security allows sharing of resources with mixed levels of security in a single image
  - Example: Single image of data sharable by multiple enterprise departments with different need to know

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%



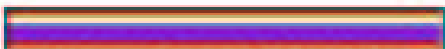
## Multilevel Security on zSeries

# 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 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.

# Recap - Multilevel Security on zSeries with DB2 V8

## □ Proven mainframe reliability and quality of service

### ➤ Self-optimizing

- Managing to business priorities:  
z/OS Workload Manager

- Managing resources:  
Intelligent Resource Director

- Managing storage: z/OS DFSMS

### ➤ Robust z/OS security:

- RACF & PKI Services
- Intrusion Detection Services
- Address Space Isolation

### ➤ zSeries cryptography

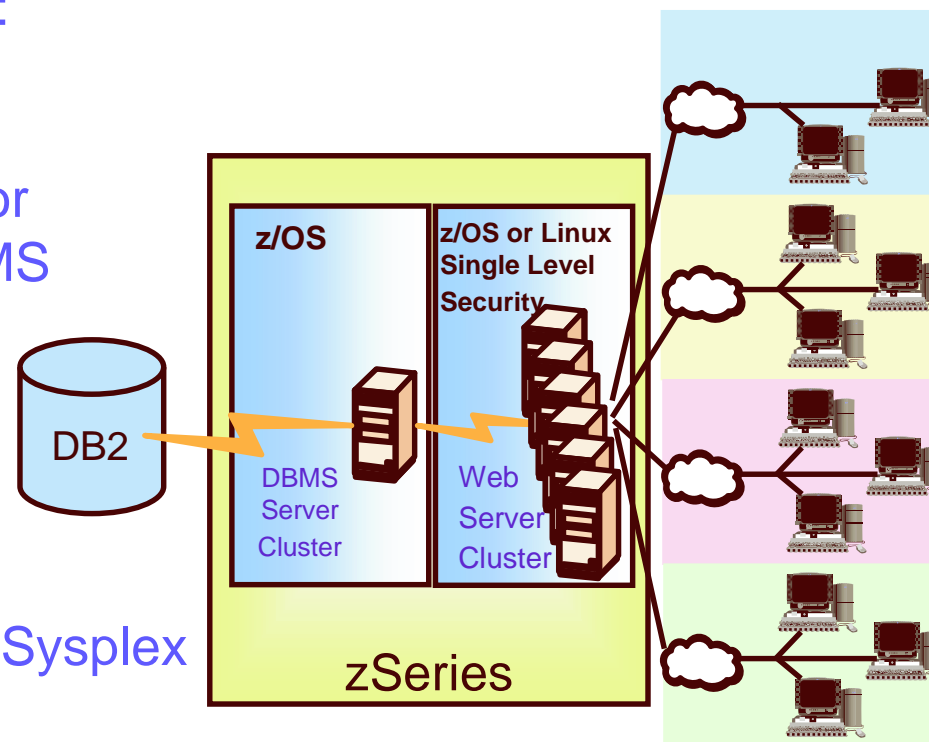
### ➤ Scale and high availability: Parallel Sysplex

### ➤ Business recovery: GDPS

(Globally Dispersed Parallel Sysplex)

### ➤ Server consolidation:

- Linux for zSeries or z/OS for Web Serving
- Secure Partitions: LPARS certified at Common Criteria EAL5



**Multilevel Security  
on zSeries**

# Establishing a Multilevel Security environment on zSeries

## ❖ Requirements

### ❑ Hardware

- z/OS V1R5 is support on the following servers:
  - z990, z900, z890, z800, G5, G6, MP3000 servers or equivalent
- DB2 v8 is supported on the following servers:
  - z990, z900, z890, z800 or equivalent

### ❑ Software

- z/OS V1R5
  - RACF
  - For System specific security labels -JES2
  - Print Services Facility (PSF)

### ❑ Sysplex (shared DASD)

- 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

❖ **NOTE:** Infoprint Server and BDT do not support Multilevel Security

# 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.