IBM Software Group

DB2 for z/OS V8 Security Enhancements

DB2 Information Management Software

ON DEMAND BUSINESS

Eric Derbanne
IBM France Software Group
eric.derbanne@fr.ibm.com

DB2 Security Needs ... Data Security

- **Data security is a top issue in today's world due to:**
  - Need for compliance with security legislation
    - Health Insurance Portability and Accountability Act of 1996 (HIPAA); Health care
    - Gramm-Leach-Bliley Act of 1999 (GLBA); Financial services
    - . . .
  - Emergence of Storage Area Networks (SANs)
    - The need for safely storing data in a widely accessible device has increased

- **DB2 Security enhancements**
  - Multilevel security for access control
    - Multilevel security with row granularity
    - Multilevel security for object level access
  - Session variables
  - Encryption built-in functions

Database Security and Granularity

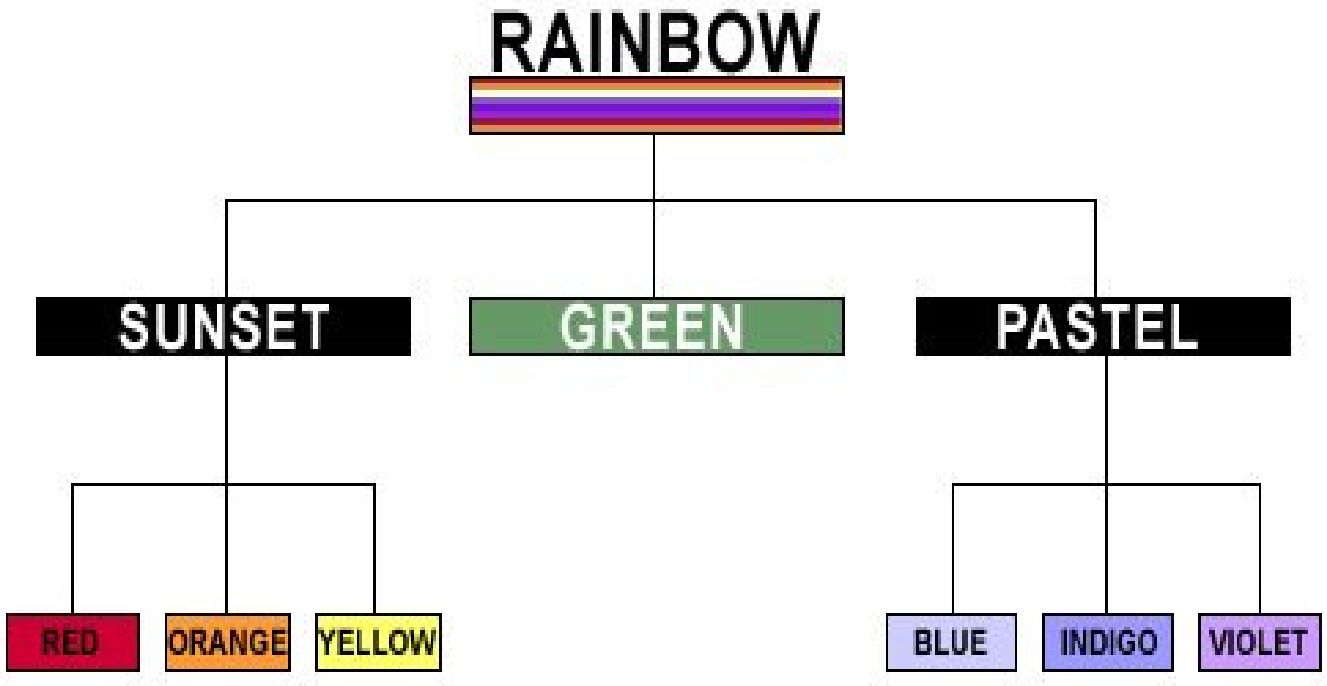
- **Low level access control is increasingly critical**
  - Web hosting
  - Privacy of data
- **Need row level granularity**
  - Individual users can be restricted to a specific set of rows
- **Need for mandatory security**
  - Not easily bypassed by high database authorization levels
- **Today, you can use views to limit access**
  - Can be cumbersome
  - Not as effective for UPDATE, INSERT, DELETE and utilities

New concepts

- **Subjects and objects**
  - Objects: "things" you try to protect
  - Subjects: "things" that need to access objects
- **Multilevel security (MLS)**
- **Security labels (SECLABEL)**
- **Mandatory access control (MAC)**
  - Governed by SECLABELs
- **Discretionary access control (DAC)**
  - Governed by access lists

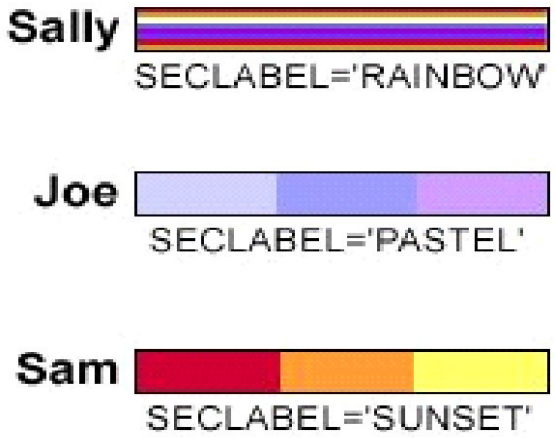
MLS with Row Granularity

- **In RACF**
  - Set up a security hierarchy (SECLEVEL) and categories (CATEGORY)
  - The SECLABEL class is active
  - Assign security labels to users
- **SECLABEL comparisons**
  - Dominance
  - Reverse dominance
  - Equivalence
  - Null
- **Read up**
- **Write down**



MLS with Row Granularity -2

- **Table column defined with AS SECURITY LABEL attribute**
- **Mandatory access control:**
  - Always checked at runtime
  - User's SECLABEL is retrieved from RACF when connecting to DB2
- **Check each new SECLABEL value that is accessed by the user**
- **SECLABEL values are cached to minimize processing time**



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

Accessing a table defined with MLS

- **SELECT -** user's Seclabel is compared to the Seclabel of the row
  - If user's Seclabel dominates the data Seclabel -> row returned
  - If user's Seclabel does not dominate -> no row returned, no error
- **INSERT**
  - Value of the Seclabel column for inserted row is set to the value of the user's Seclabel
  - If user has write-down authority, the user is allowed to set the Seclabel field
- **UPDATE -** user's Seclabel is compared to the Seclabel of the row to be updated
  - If the Seclabels are equivalent -> row is updated
    - Value of the Seclabel in the updated row is set to the value of the user Seclabel
  - If user has write-down authority, then down-level rows can be accessed and updated
- **DELETE -** user's Seclabel is compared to the Seclabel of the row to be deleted
  - If the Seclabels are equivalent -> row is deleted
  - If user has write-down authority, then down-level rows can be accessed and deleted

Multilevel Security and Utilities

- **LOAD RESUME** of a table space containing tables with multilevel security (MLS) with row granularity
  - User must be identified to RACF and have a valid ACEE
  - Rules for LOAD RESUME are similar to the rules for INSERT
  - Without write-down, Seclabel set to user's current Seclabel
  - With write-down permission, permitted to specify a Seclabel
- **LOAD REPLACE** on a MLS table space requires write-down authority
- **UNLOAD** and **REORG UNLOAD EXTERNAL**
  - User must be identified to RACF and have a valid ACEE
  - Similar to the rules for SELECT statements
  - Only rows can be unloaded if the user's seclabel dominates the data seclabel
  - No error returned if this is not true, only the row is not unloaded

Multilevel Security and Utilities -2

- **REORG ... DISCARD** of tables
  - User must be identified to RACF and have a valid ACEE
  - For each row unloaded from those tables, if the row qualifies to be discarded, the user Seclabel is compared to the data Seclabel
    - If they are the same -> row discarded
    - If they are not the same -> check for equivalence of the two seclabels
      - If equivalent -> row discarded
      - If not check if write-down privilege is in effect:
        - In effect and user had write-down -> row discarded if user seclabel dominates the row
        - In effect and user does not have write-down -> not discarded
        - Write-down not in effect -> dominance is enough

Requirements and Restrictions

- **Requirements**
  - Requires z/OS 1.5 and Security Server (RACF) V1R5
- **Restrictions**
  - Row level security is not enforced for referential constraints
  - Referential constraints cannot be defined on a seclabel column
  - Sysplex parallelism is not used for queries on a table defined with a security label
  - As mentioned before, the seclabel column cannot have
    - FIELDPROC, EDITPROC, check constraints
  - Trigger transition tables do not have security labels
  - Global temporary tables cannot have a true Seclabel column
  - Some additional restrictions for MQTs

DB2 Command Control Improved

- **DB2 commands – using GRANTs**
  - When signed on console, jobs, TSO SDSF, …
    Signed on id used, rather than SYSOPR
  - Need to GRANT proper authorization e.g. SYSOPR, DISPLAY, …
- **Options for commands (secondary ids are new)**
  - Grant access to primary or secondary authids
  - Grant access to public
  - Use exit or RACF authorization control for commands
- **DB2 commands – using RACF access control**
  - When signed on console, jobs, TSO, …
    Signed on id used, rather than SYSOPR
  - Need to provide proper authorization, using PERMIT or GRANT, users, groups, ...
- **WebSphere environment**
- **Multilevel security for object access control**

Multilevel Security for Access Control

- **MLS with RACF access control at the DB2 object level**
  - Define Seclabels for all DB2 related RACF classes and assign them to profiles
    - DSN*, MDSN* and GDSN* general resource classes
    - Respect DB2 object hierarchy (database > table space > table > row, ...)
  - Assign Seclabels to users
  - Activate SECLABEL checking and potentially write-down
  - Activate RACF access control for DB2 (DSNX@XAC)

MLS options	Security at object level	Security at row level
DB2 access control	✗	✓
RACF access control	✓	✓

- **MLS with DB2 access control and row granularity**

Multilevel security for RACF Access Control

- **Ability to use multilevel security with RACF access control for objects: views, tables, databases, …**
- **Use security profile definitions, not PERMITs**
- **Ship access control authorization exit with DB2**
  - prefix.SDSNSAMP instead of SYS1.SAMPLIB
- **Requires z/OS V1R5 & Security Server V1R5**
- **Multilevel DB2 Authorization Hierarchy for DB2 objects (subsystem or data sharing group)**

  - Database
    - Table Space
    - Table
    - Column
    - Row
  - View
  - Storage Group
  - Bufferpool
  - ...
  - Plan
  - Collection
    - Package
  - Schema
    - Stored Procedure, User-Defined Function
    - Java ARchive (JAR)
    - Distinct Type
    - Sequence

Session Variables

- **Variables set by DB2, connection or sign-on exit**
- **Built in function to retrieve value for a variable**
  - Use function in views, triggers, stored procedures, and constraints to enforce security policy
- **Can have more general, flexible access checks**
  - Multiple columns, AND/OR logic, ...
- **Complements other security mechanisms**

```
CREATE VIEW V1 AS SELECT *
FROM T1
WHERE COL5 = GETVARIABLE(SYSIBM.SECLABEL);
```

Views with Multilevel Security, Session Variables, ...

```
CREATE VIEW SW_CUSTOMER AS
  SELECT CUST_NBR, CUST_NAME, CUST_CREDIT
    FROM  CUSTOMER WHERE CUST_REGION='SW'
```

- **Views can provide only equivalent seclabel data**
- **Views can have lower seclabel than tables**
  - Eliminate protected data: rows and/or columns
  - Join or union with other tables to add or remove information
  - Use triggers, stored procedures, constraints and with check option for update control at row level
- **Views can use plan or package, Seclabel, site-defined comparisons with special registers & session variables**

Session Variables & New Special Registers

- **Session Variables**
  - Set by DB2 SYSIBM.varname
    - PLAN_NAME
    - PACKAGE_SCHEMA
    - SECLABEL
    - VERSION DATA_SHARING_GROUP_NAME
    - SYSTEM_ASCII_CCSID EBCDIC UNICODE
    - PACKAGE_NAME
    - PACKAGE_VERSION
    - SYSTEM_NAME
  - Set by connection & signon exits
    - Up to 10 variables SESSION.varname

- **Special registers**
  - Client information for this connection
    - Provided by sqleseti, Java methods, RRS SIGNON & SET_CLIENT_ID
    - CLIENT_ACCTNG accounting string
    - CLIENT_APPLNAME value of application name
    - CLIENT_USERID client user ID
    - CLIENT_WRKSTNNAME workstation name

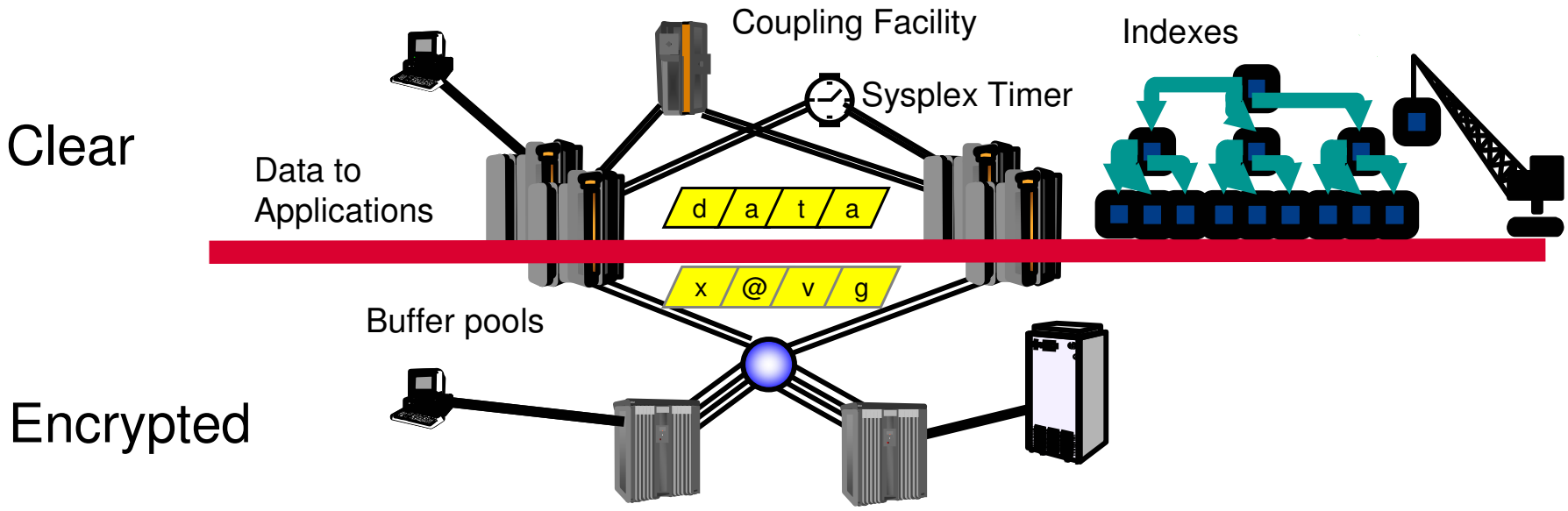
DB2 and Encrypted Data

- What do you want to protect ? from whom ?
- Techniques, where to encrypt / decrypt

Outside of DB2	General, flexible, no relational range comparisons FOR BIT DATA
DB2 FIELDPROC	No relational range comparisons, FIELDPROC restrictions, FOR BIT DATA
DB2 EDITPROC	indexes are not encrypted, EDITPROC restrictions
User-defined function	General, flexible, invocation needed, no relational range comparisons
Stored procedure	General, flexible, invocation needed, no relational range comparisons
SQL functions	General, flexible, invocation needed, no relational range comparisons

IBM Tool for DB2 EDITPROC and IMS Encryption

- **Data encryption on disk, data at rest**
  - Data on channel, in buffer pools are encrypted
  - Data to applications & indexes are not encrypted
- **Existing authorization controls are unaffected**



V8 Built-in Functions for Encryption

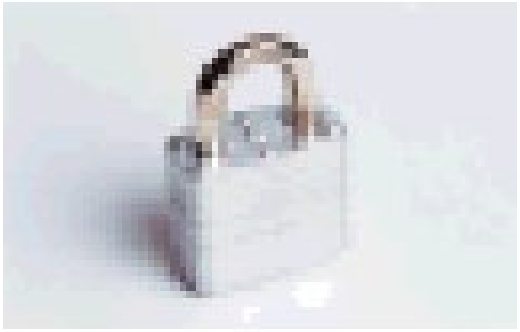
- **ENCRYPT_TDES encrypt a column in a table with a user-provided encryption password**
- **ENCRYPTION PASSWORD special register**
- **DECRYPT_BIT, DECRYPT_CHAR, DECRYPT_DB**
- **GET_HINT obtain hint to help remember ENCRYPTION PASSWORD**
- **GENERATE_UNIQUE creates CHAR(13) FOR BIT DATA value that is unique across Sysplex**
- **DRDA encryption on the wire**

Return Authid Information

- **APAR PQ47973 in V6 & V7**
- **READS IFI Call to retrieve**
  - Primary AUTHID USER
  - SQL AUTHID CURRENT SQLID
  - SECONDARY AUTHIDs
- **IFCID 234 maps the information**
- **QMF V7.2 LIST TABLES**
  - works with authority groups defined by DB2 secondary authorization IDs.

Summary of DB2 for z/OS V8 Security

- **Very significant changes for increased**
  - Security
  - Flexibility
  - Integration
  - Ease of use for safe security
  - Assurance



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)
    - http://publibz.boulder.ibm.com/epubs/pdf/e0z2e100.pdf
- **RACF presentations, MLS and others**
  - http://www.ibm.com/servers/eserver/zseries/zos/racf/presentations.html
- **RACF web site:**
  - http://www.ibm.com/servers/eserver/zseries/zos/racf

References

- **DB2 UDB for z/OS publications:**
  - Administration Guide, SC18-7413
  - Command Reference, SC18-7416
  - Data Sharing: Planning and Administration, SC18-7417
  - Installation Guide, GC18-7418-00
  - RACF Access Control Module Guide and Reference Version 8, SA22-7938
  - SQL Reference, SC18-7426
  - Utility Guide & Reference, SC18-7427
  - DB2 Version 8: Everything you wanted …, SG24-6079
- **DB2 information web site:**
  - http://www.ibm.com/software/data/db2/zos/v8books.html

More information on DB2 UDB for z/OS web site

- **ibm.com/software/db2zos**
  - primary home page
- **ibm.com/software/db2zos/support.html**
  - Click on Support for much more information
  - Technotes, presentations, Redbooks, …
- **ibm.com/software/db2zos/v8books.html**
  - Many books on DB2 UDB for z/OS Version 8
- **ibm.com/software/data/db2imstools**
  - Encryption tool EDITPROC
- **ibm.com/developerworks/db2**
  - programmer information