Oracle MAC/Labels

Group 5

Our Team

Luu Chan Hung

Dang Cao Cuong

Nguyen Thanh Chuong

Nguyen Thanh Hung

Phan Tuan Khai

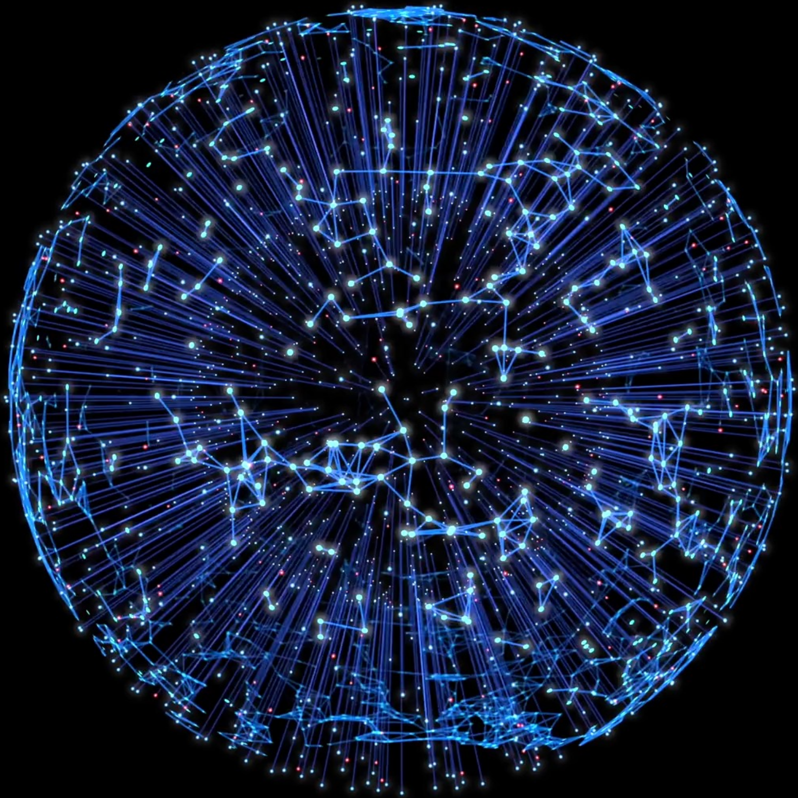


TABLE OF CONTENTS

01 ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

03 LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

04 ORACLE LABEL SECURITY

05 DEMONSTRATION

06 SUMMARY

01

ACCESS CONTROL

MANDATORY ACCESS CONTROL

01 ACCESS CONTROL

MANDATORY ACCESS CONTROL

DEFINITION

The security mechanism of a DBMS must include provisions for restricting access to the database system

TECHNOLOGY

Discretionary Access Control
Mandatory Access Control
Role-Based Access Control

02

ACCESS CONTROL

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ACCESS CONTROL

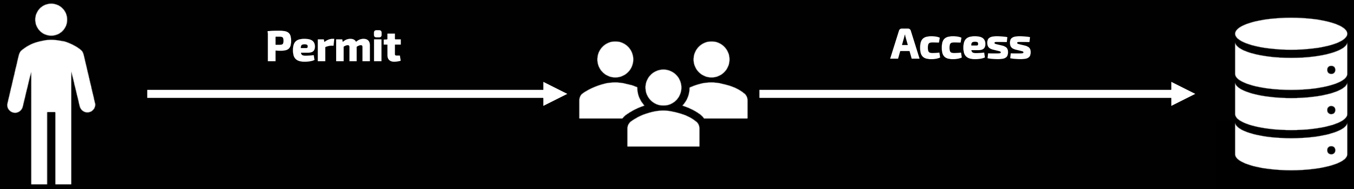
02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

WHY DO WE NEED ?

DAC

An all-or-nothing method : A user either has or does not have a certain privilege



Permit

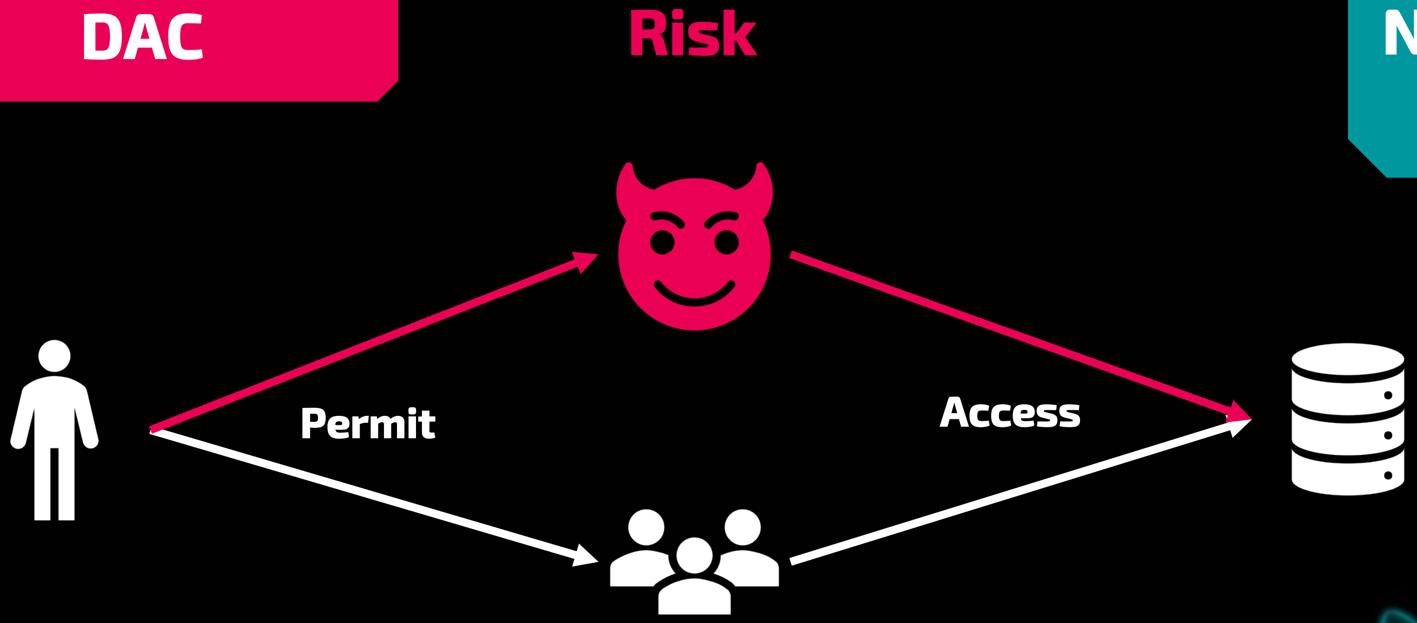
Access

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

WHY DO WE NEED ?

DAC



ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

WHY DO WE NEED ?

DAC

Risk

↓

Need an additional security policy to classifies data and users based on security classes

02 MANDATORY ACCESS CONTROL

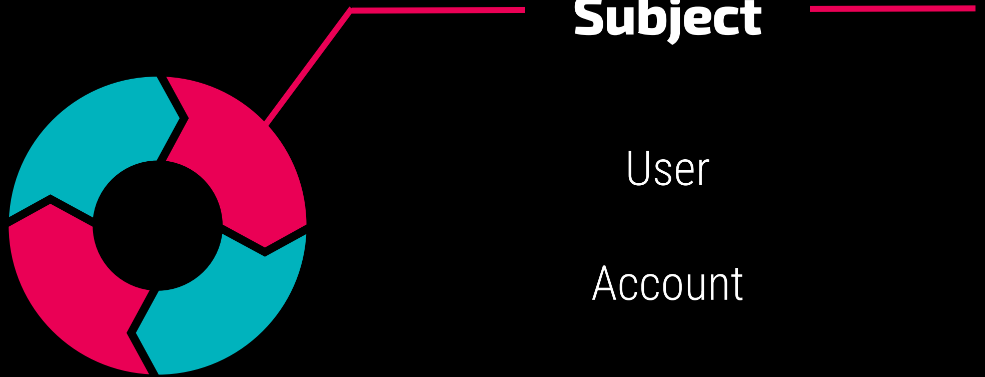
LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

MAC

An access control mechanism based on label relationships

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL



Mechanism

Subject

User

Account

Program

Object

Relation

Tuple

Column

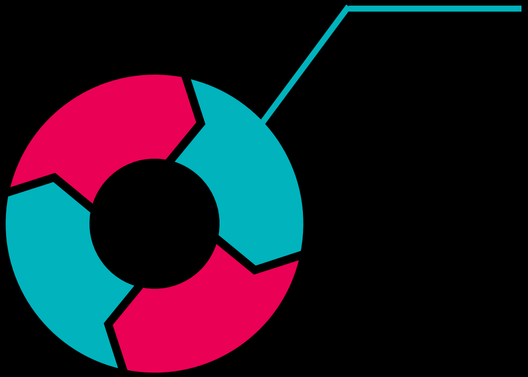
View

Operation

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL



Clearance

Classify our subject/object into different security level

Typical security classes

- Top Secret (TS)
- Secret (S)
- Confidential (C)
- Unclassified (U)

Mechanism

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Mechanism

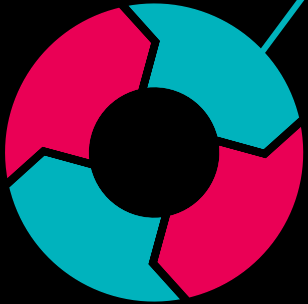
Bell-LaPadula model

Classify each subject and object into one of the security classifications TS, S, C, or U

⇒ The clearance (classification) of a subject S as class(S) and to the classification of an object O as class(O)

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL



Mechanism

Restrictions rule

Simple security property

Class(S) < class(O)

$$\text{Subject S} \xrightarrow{\text{No read access}} \text{Object S}$$

Star property (or *-property)

Class(S) > class(O)

$$\text{Subject S} \xrightarrow{\text{No write access}} \text{Object S}$$

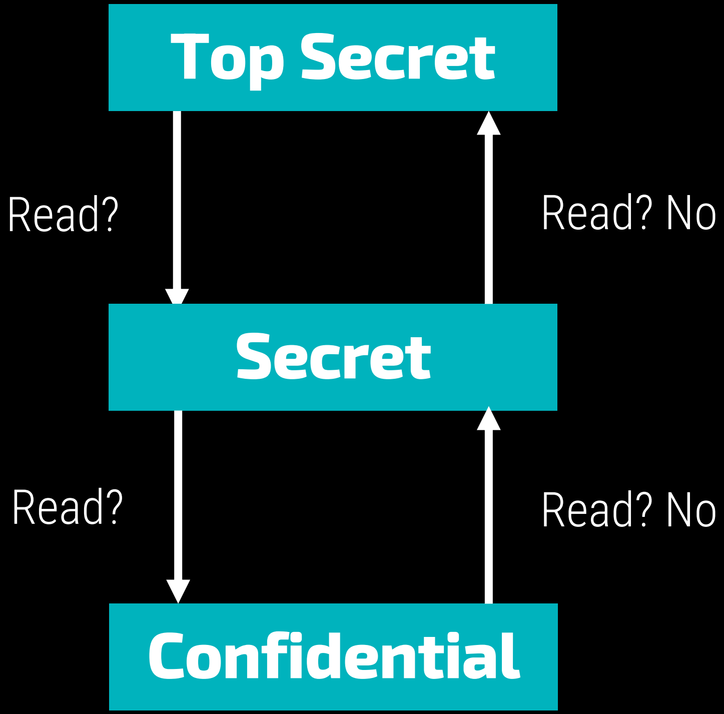
02

ACCESS CONTROL

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



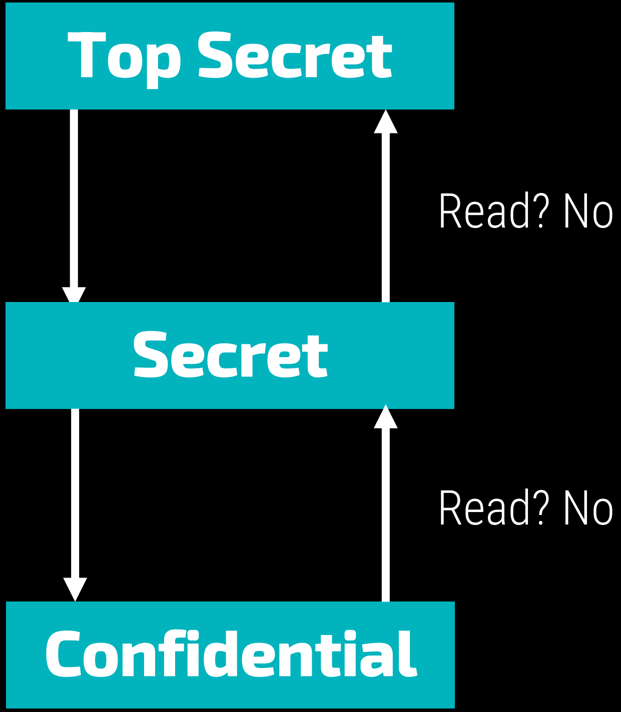
ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules

Read down?
Yes!


Top Secret

Read? No

Secret

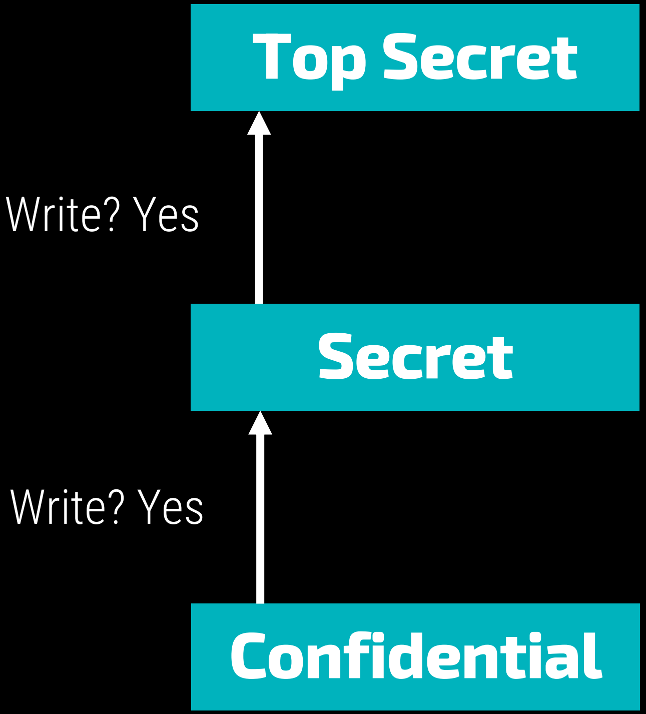
Read? No

Confidential

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules

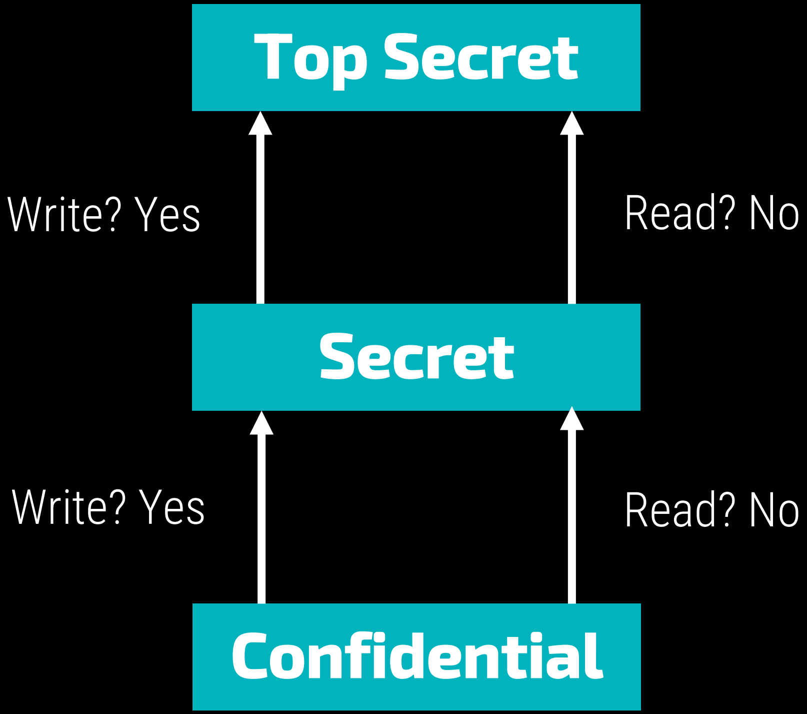


ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



Top Secret

Write? Yes

Read? No

Secret

Write? Yes

Read? No

Confidential

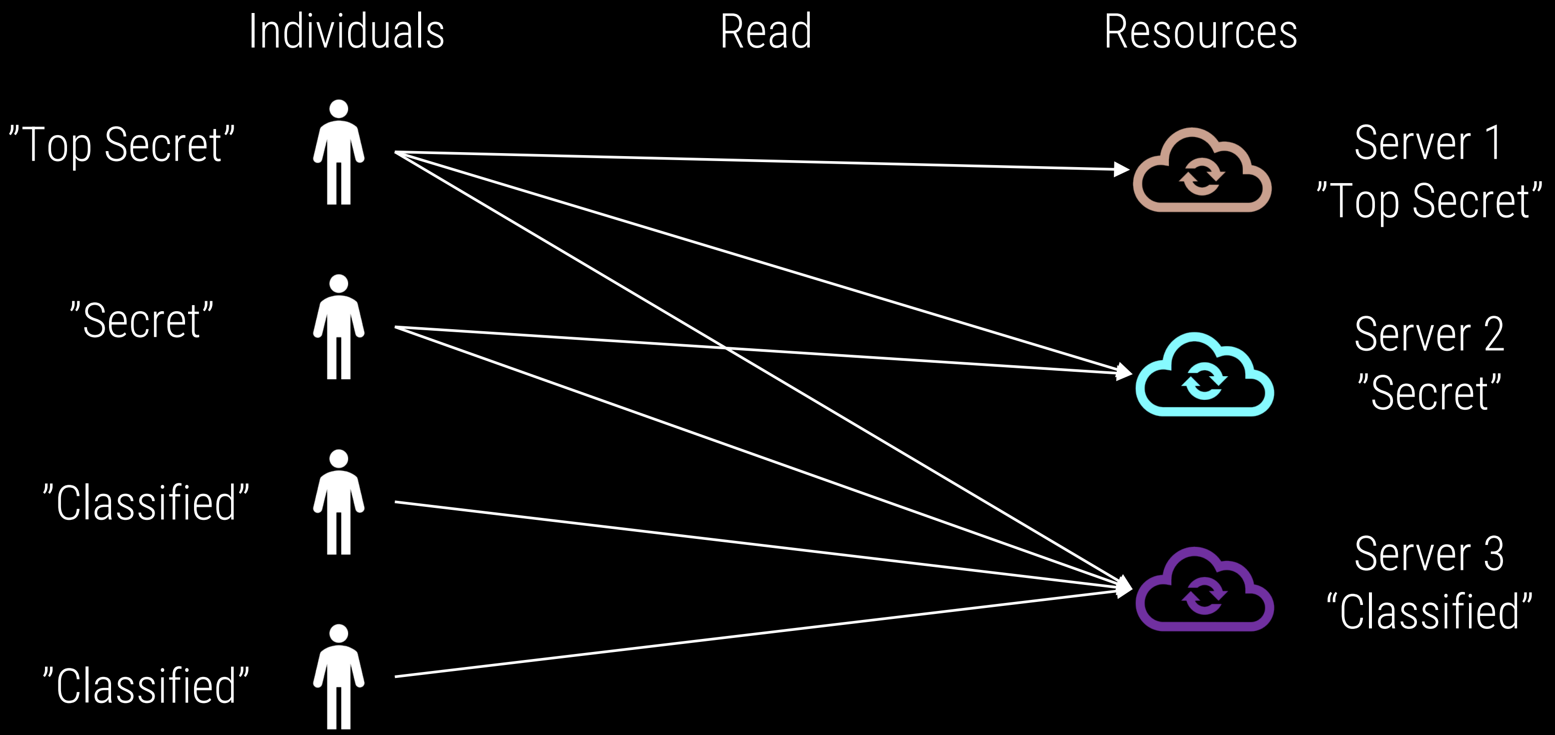
02

ACCESS CONTROL

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



Individuals

Read

Resources

"Top Secret"

"Secret"

"Classified"

"Classified"

Server 1
"Top Secret"

Server 2
"Secret"

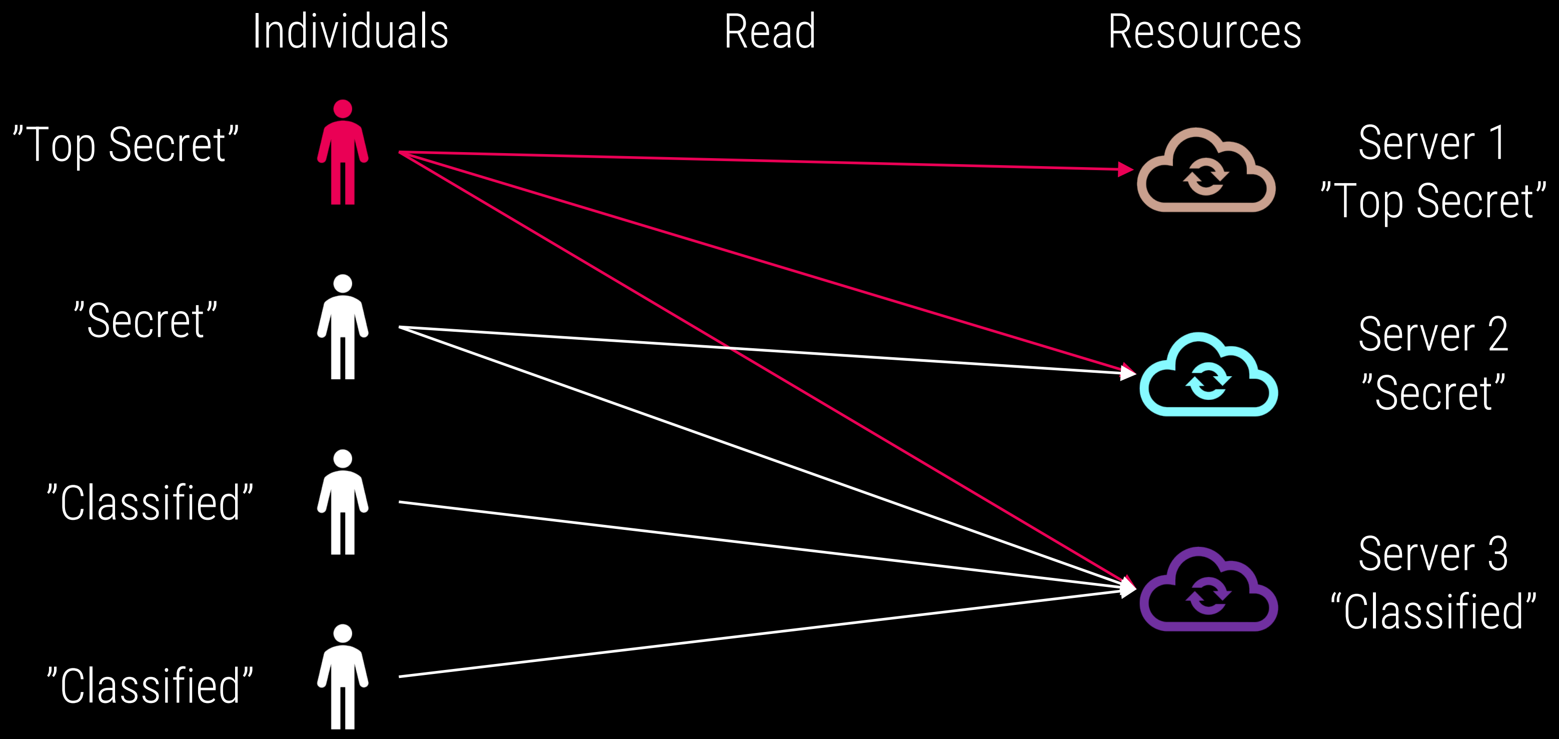
Server 3
"Classified"

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



Individuals

Read

Resources

"Top Secret"

"Secret"

"Classified"

"Classified"

Server 1 "Top Secret"

Server 2 "Secret"

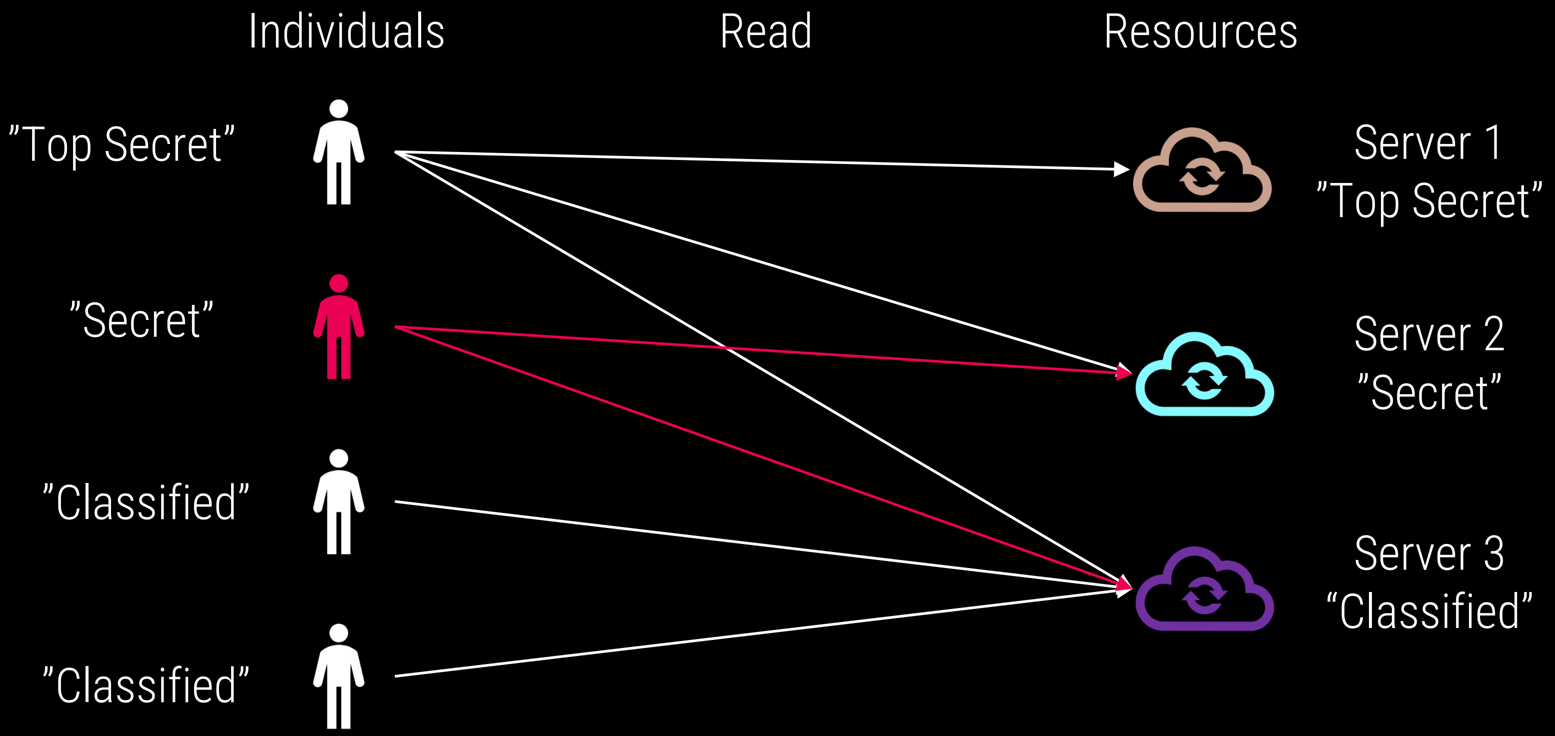
Server 3 “Classified”

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



Individuals

Read

Resources

”Top Secret”

”Secret”

”Classified”

”Classified”

Server 1 ”Top Secret”

Server 2 ”Secret”

Server 3 “Classified”

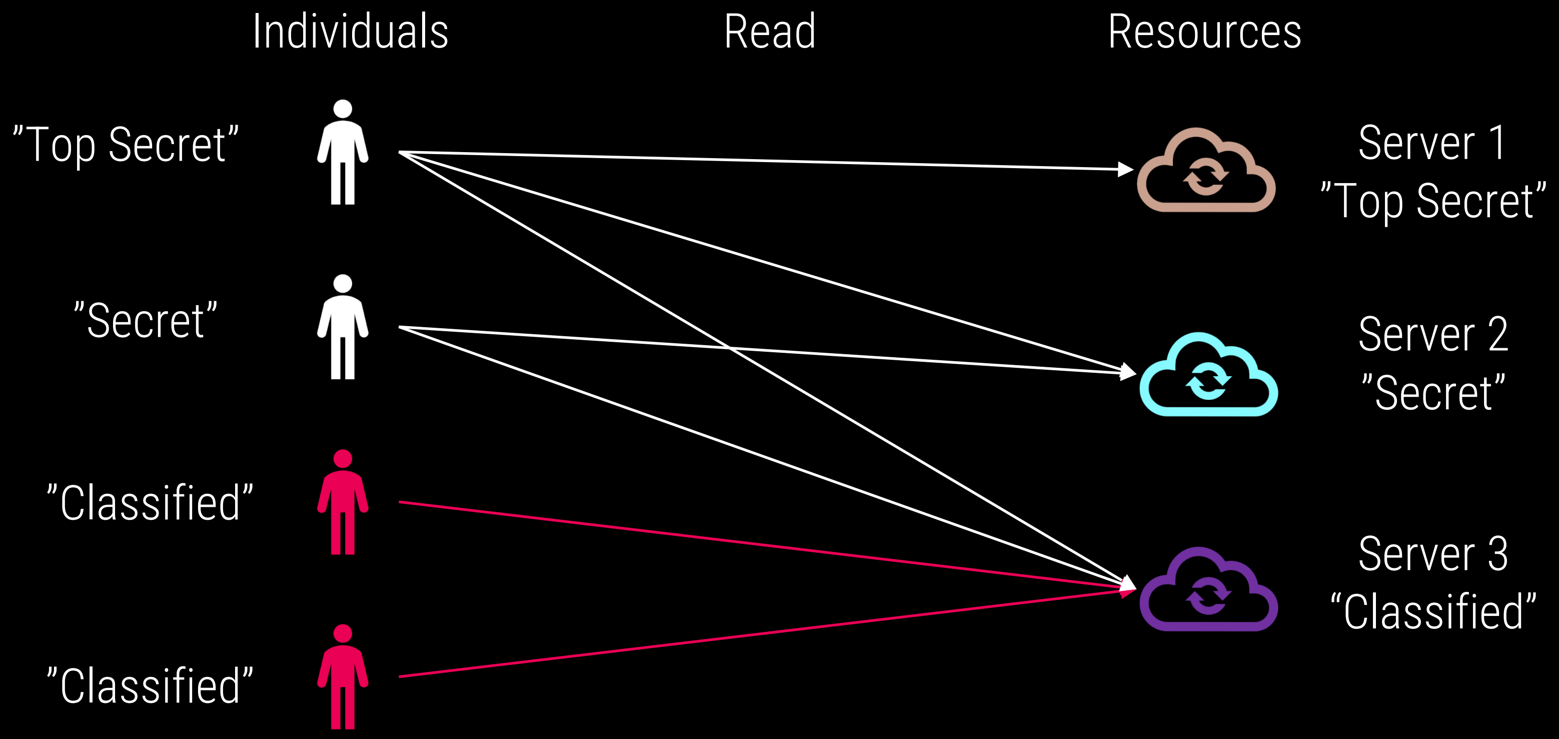
02

ACCESS CONTROL

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Demonstration of MAC rules



Individuals

Read

Resources

”Top Secret”

”Secret”

”Classified”

”Classified”

Server 1
”Top Secret”

Server 2
”Secret”

Server 3
“Classified”

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Purpose

Classification attribute C

To incorporate multilevel security notions into the relational database model

**Consider attribute values and tuples as data objects

Multilevel Relation

02

ACCESS CONTROL

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Purpose

Classification attribute C

Tuple classification attribute TC

Schema:

Each attribute A --- associated --- a classification attribute C

Value:

Each attribute value in a tuple is associated with a corresponding security classification.

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Classification attribute C

Tuple classification attribute TC

Multilevel model

Each tuple --- provided --- a tuple classification

TC = max (all classification attributes C in a tuple)

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Tuple classification attribute TC

Multilevel model

The model that allows classifications at multiple security levels

Apparent key

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Tuple classification attribute TC

Multilevel model

Apparent key

Classifications at multiple security levels

Schema R with n attributes

$$R(A_1,C_1,A_2,C_2,\ldots,A_n,C_n,TC)$$

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Tuple classification attribute TC

Multilevel model

Apparent key

Classifications at multiple security levels

Schema R with n attributes

$$R(A_1,C_1,A_2,C_2,\ldots\ ,A_n,C_n,TC)$$

C_i = classification attribute associated with attribute A_i

Multilevel Relation

MANDATORY ACCESS CONTROL

Tuple classification attribute TC

Multilevel model

Apparent key

Multilevel Relation

Classifications at multiple security levels

Schema R with n attributes

$$R(A_1,C_1,A_2,C_2,\ldots,A_n,C_n,TC)$$

C_i = classification attribute associated with attribute A_i

TC = the tuple classification attribute

-> provides a general classification for the tuple

Multilevel model

Apparent key

Filtering

The apparent key of a multilevel relation is the set of attributes that would have formed the primary key in a regular (single-level) relation

Multilevel Relation

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Apparent key

Filtering

Polyinstantiation

- Store a single tuple in the relation at a higher classification level -> produce the corresponding tuples at a lower-level classification
- Null values for attribute values whose security classification > the user's security clearance

Multilevel Relation

MANDATORY ACCESS CONTROL

Filtering

Polyinstantiation

Example 1

Store two or more tuples at different classification levels with the same value for the apparent key

⇒ Several tuples can have the same apparent key value but have different attribute values for users at different clearance levels.

■■■■■■■□□□

Multilevel Relation

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Polyinstantiation

Example 1

Integrity Rules

Enter

Multilevel Relation

Example 1

Name	Salary	Job Performance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

- Classification attribute values next to each attribute's value
- Assume that the Name attribute is the apparent key, and consider the query SELECT * FROM EMPLOYEE

Example 1

Name	Salary	Job Performance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

Name	Salary	Job Performance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

Security clearance S

Same with the original table

Example 1

Name	Salary	Job Performance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

Name	Salary	Job Performance	TC
Smith U	40000 C	NULL C	S
Brown C	NULL C	Good C	S

Security clearance C

Cannot see the value: Salary of 'Brown' & JobPerformance of 'Smith'

Example 1

Name	Salary	Job Performance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

Name	Salary	Job Performance	TC
Smith U	NULL U	NULL U	U

security clearance U

Only the Name attribute of 'Smith' to appear

ACCESS CONTROL

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Polyinstantiation

Example 1

Integrity Rules

End of Example 1

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Example 1

Integrity Rules

Example 2

Entity integrity

Apparent key

- must not be null
- must have the same security classification within each individual tuple.

Other attribute values

- must have a security classification ≥ that of the apparent key

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Example 1

Integrity Rules

Example 2

Null integrity and interinstance integrity

- Ensure that if a tuple value at some security level can be filtered (derived) from a higher-classified tuple, then it is sufficient to store the higher-classified tuple in the multilevel relation.

Multilevel Relation

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Integrity Rules

Example 2

Enter

Multilevel Relation

Example 2

Name		Salary		Job_ Performance		TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S

```
UPDATE    EMPLOYEE
SET       Job_Performance = 'Excellent'
WHERE     Name = 'Smith'
```

Name		Salary		Job_ Performance		TC
Smith	U	40000	C	Fair	S	S
Smith	U	40000	C	Excellent	C	C
Brown	C	80000	S	Good	C	S

- Lower security clearance could write to higher security clearance
- Override is not allowed
- ➢ Create an additional tuple at the lower classification level C
- The basic update operations of the relational model (INSERT, DELETE, UPDATE) must be modified to handle this and similar situations

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Integrity Rules

Example 2

End of
Example 2

Multilevel Relation

02 MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

Advantage

Mandatory policies ensure a high degree of protection

Suitable for military and high-security types of applications

Disadvantage

Too rigid

Applicable to few environments

Additional burden of labeling every object with its security classification.

03

MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

03

MANDATORY ACCESS CONTROL

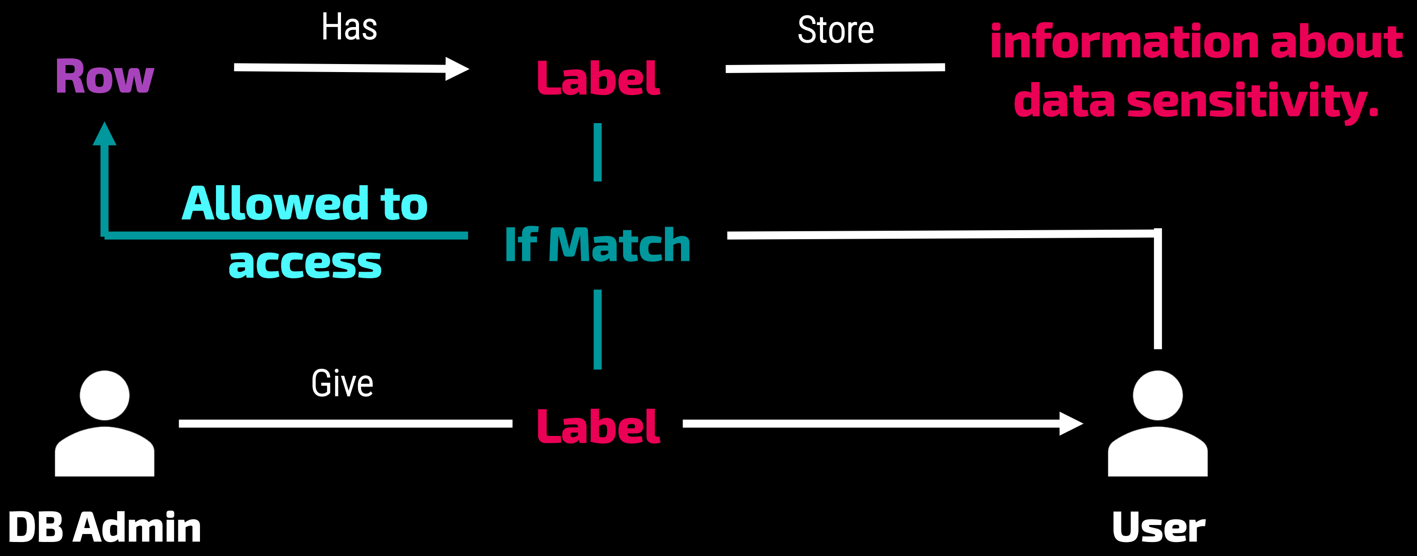
LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

Row-level access control

Label security policy

Considering the data row by row.



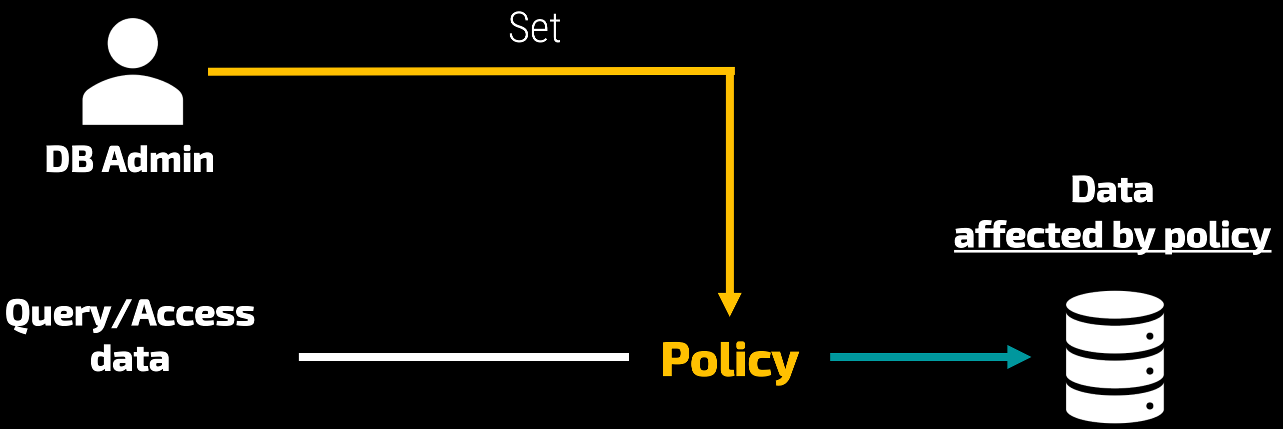
MANDATORY ACCESS CONTROL

03 LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

Row-level access control

Label security policy



03

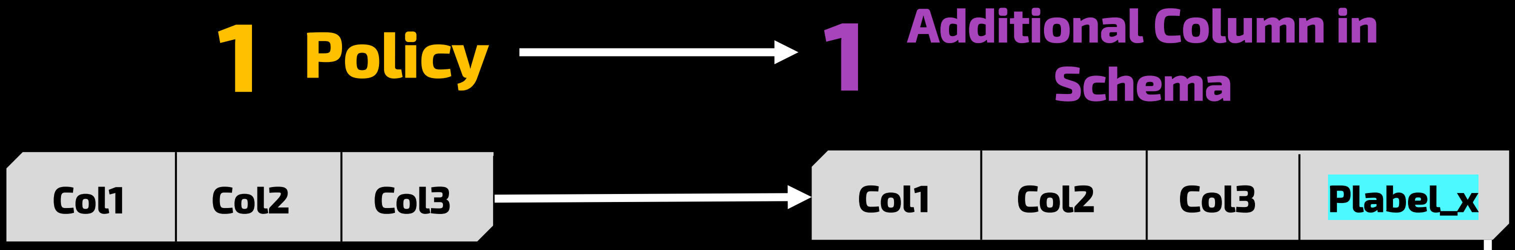
MANDATORY ACCESS CONTROL

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

Row-level access control

Label security policy



Contains the label

The DBA: set an initial default row label

The user: write the label

- Value = the user’s minimum level to the user’s current session label

04

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

DEMONSTRATION

04 ORACLE LABEL SECURITY

DEMONSTRATION

Purpose

- Restricting access to entire tables or isolating sensitive data into separate databases is a costly operation to administer

⇒ Oracle Label Security function of Oracle Database overcomes the need for such measures by enabling row-level access control

- Built on Virtual Private Database (VPD) Technology

Virtual Private Database (VPD) Technology

Add predicates to user statements to limit their access in a transparent manner to the user and the application

These VPD policies enforce object level access control or row-level security

Virtual Private Database (VPD) Technology

Add predicates to user statements to limit their access in a transparent manner to the user and the application

These VPD policies enforce object level access control or row-level security

VPD provides an application programming interface (API) that allows security policies to be attached to database tables or views using PL/SQL

Virtual Private Database (VPD) Technology

These VPD policies enforce object level access control or row-level security

VPD provides an application programming interface (API) that allows security policies to be attached to database tables or views using PL/SQL

The policy function returns a predicate (a WHERE clause) that is then appended to the user's SQL statement, thus transparently and dynamically modifying the user's data access.

ORACLE LABEL SECURITY

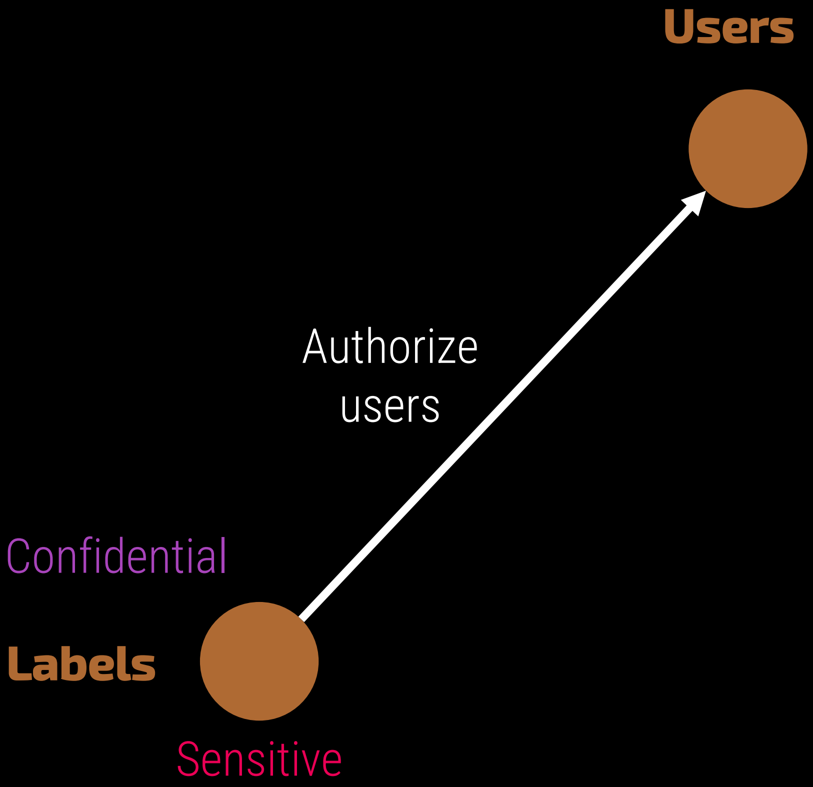
Virtual Private Database (VPD) Technology

VPD provides an application programming interface (API) that allows security policies to be attached to database tables or views using PL/SQL

The policy function returns a predicate (a WHERE clause) that is then appended to the user's SQL statement, thus transparently and dynamically modifying the user's data access.

ORACLE LABEL SECURITY

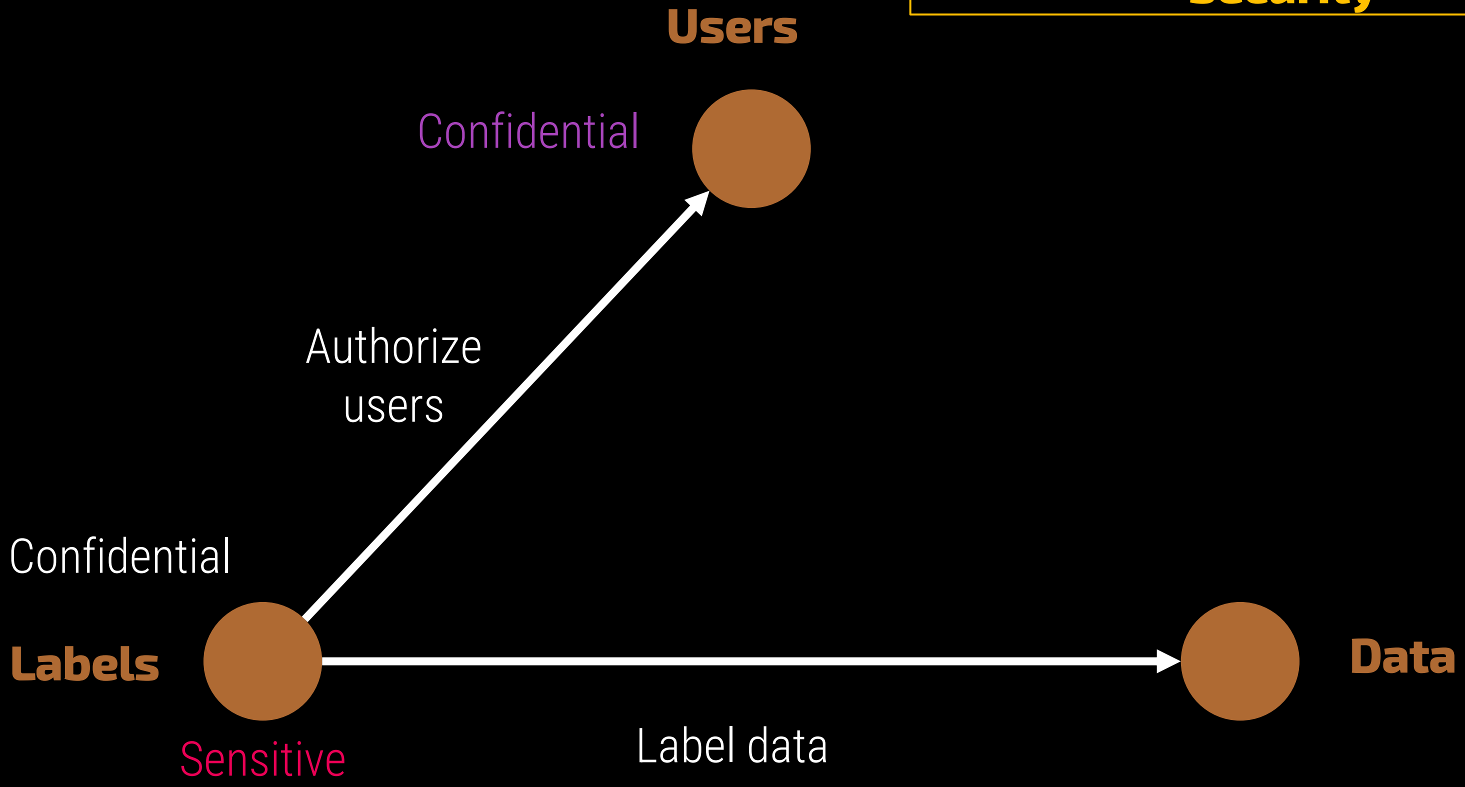
Mechanism of Oracle Label Security



ORACLE LABEL SECURITY

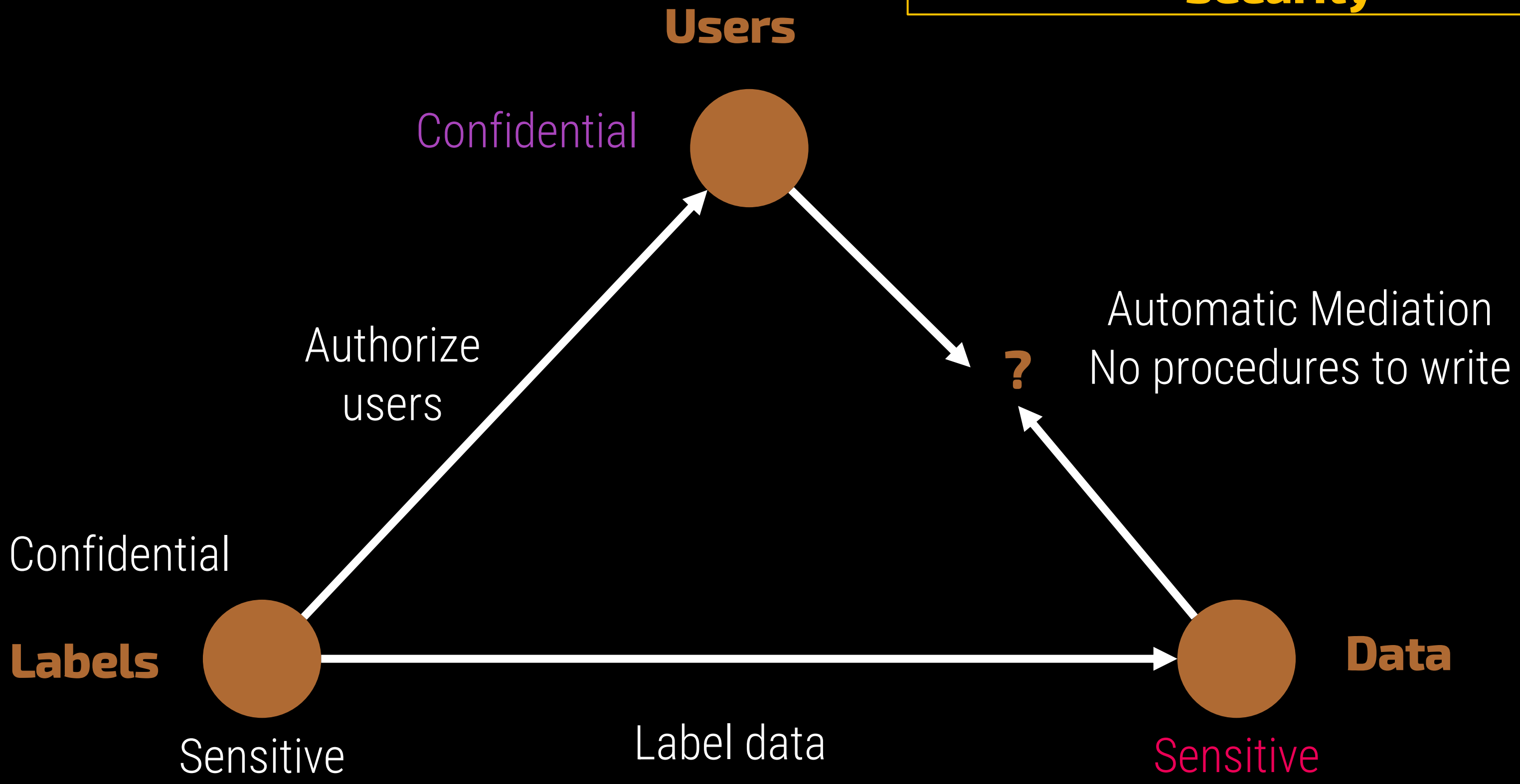
DEMONSTRATION

Mechanism of Oracle Label Security



ORACLE LABEL SECURITY

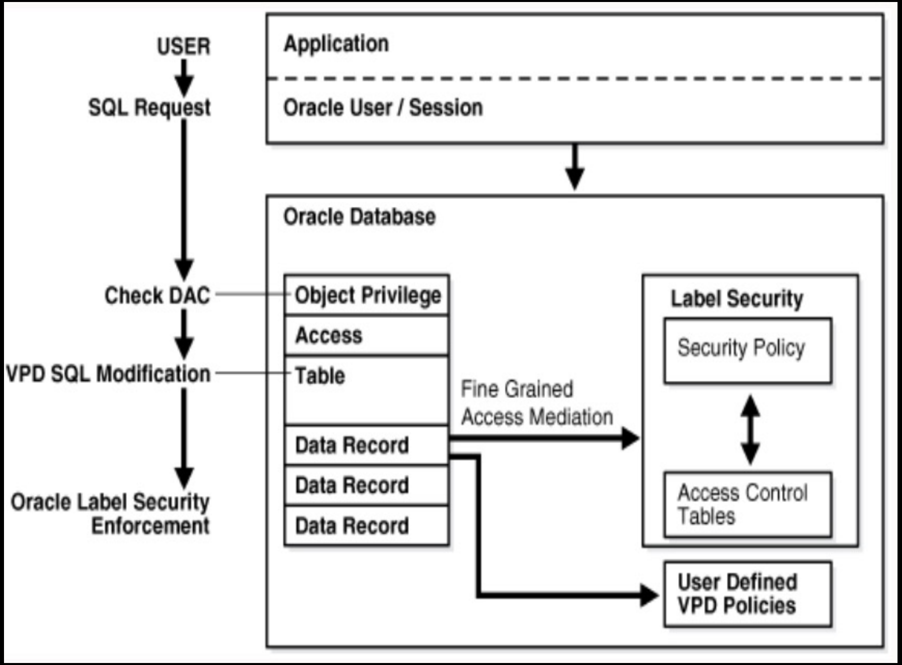
Mechanism of Oracle Label Security



ORACLE LABEL SECURITY

DEMONSTRATION

Architecture



1. An application user in an Oracle Database session sends a SQL request to query a table.

04

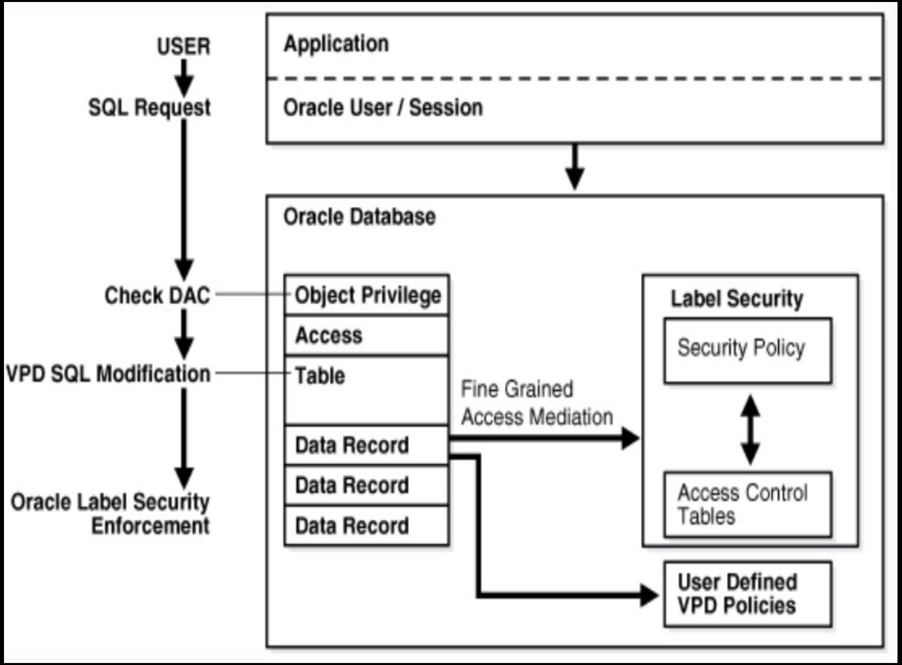
LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

ORACLE LABEL SECURITY

DEMONSTRATION

I II III **IV** V VI

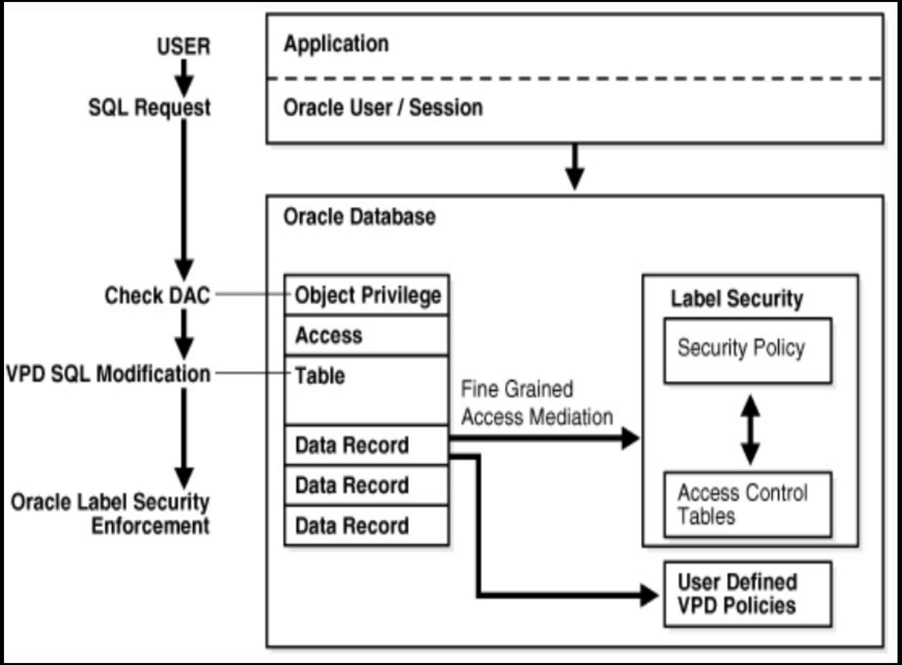
Architecture



1. An application user in an Oracle Database session sends a SQL request to query a table.

2. Oracle Database checks the user's data access control (DAC) privileges for performing a SELECT statement on the table.

Architecture



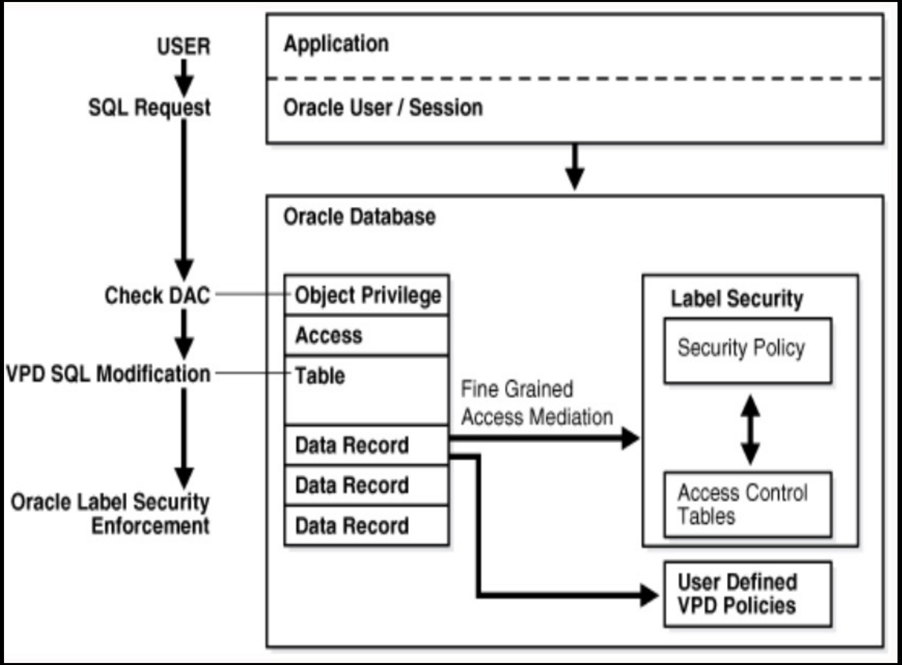
2. Oracle Database checks the user's data access control (DAC) privileges for performing a SELECT statement on the table.

3. User have the appropriate privileges ?
-> Oracle Database checks if there are any Oracle Virtual Private Database (VPD) policies attached to the table.

ORACLE LABEL SECURITY

DEMONSTRATION

Architecture



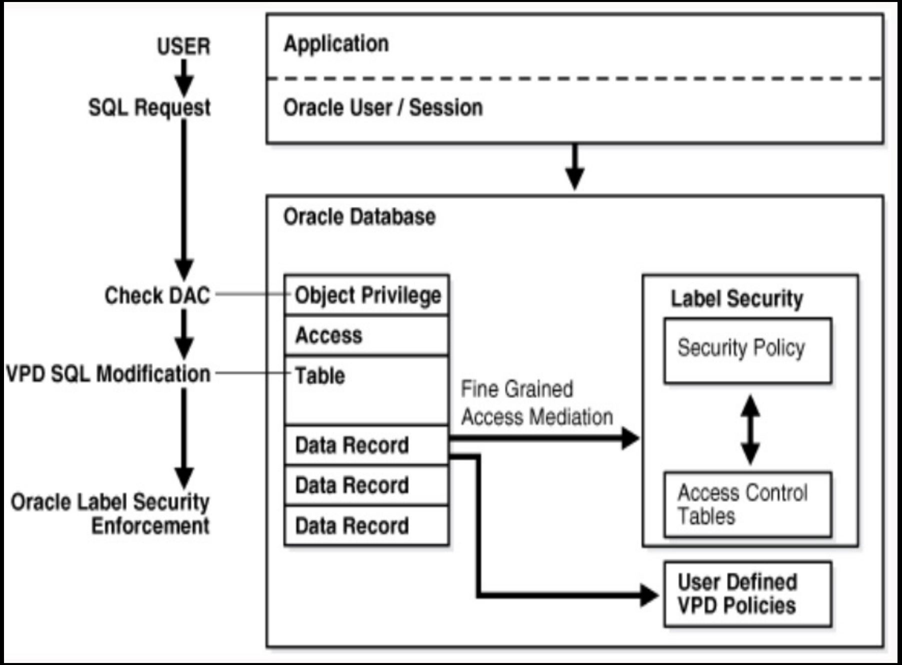
3. User have the appropriate privileges ?
-> Oracle Database checks if there are any Oracle Virtual Private Database (VPD) policies attached to the table.

4. Oracle Database then checks if there are any Oracle Label Security policies that are assigned to the table.

ORACLE LABEL SECURITY

DEMONSTRATION

Architecture



4. Oracle Database then checks if there are any Oracle Label Security policies that are assigned to the table.

5. OLS compares the labels assigned to individual rows with the users' label authorizations
-> Allow or deny access.
The session label is based on label authorizations that are assigned to the user.

Components of Oracle Label Security

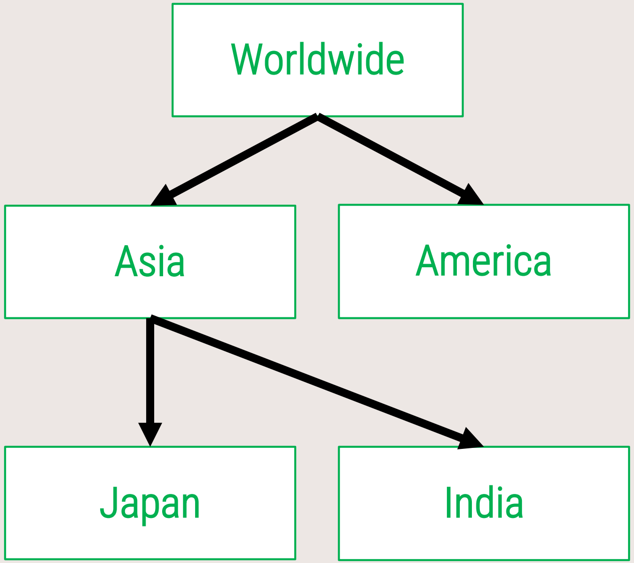
Level

- Highly Sensitive
- Sensitive
- Confidential
- Public

Compartment

- Project A
- Project D
- Project B
- Project E
- Project C

Group



Components of Oracle Label Security

Component	Description	Example

Level	A single specification of the sensitivity of labeled data within the ordered ranks established	`CONFIDENTIAL(1),`
		`SENSITIVE(2),`
		`HIGHLY_SENSITVE(3)`

Compartments	Zero or more categories associated with the labeled data	`FINANCIAL, STRATEGIC,`
		`NUCLEAR`

Groups	Zero or more identifiers for organizations owning or accessing the data	`EASTERN_REGION` `WESTERN_REGION`

VI

EXAMPLE 3

EXAMPLE 3

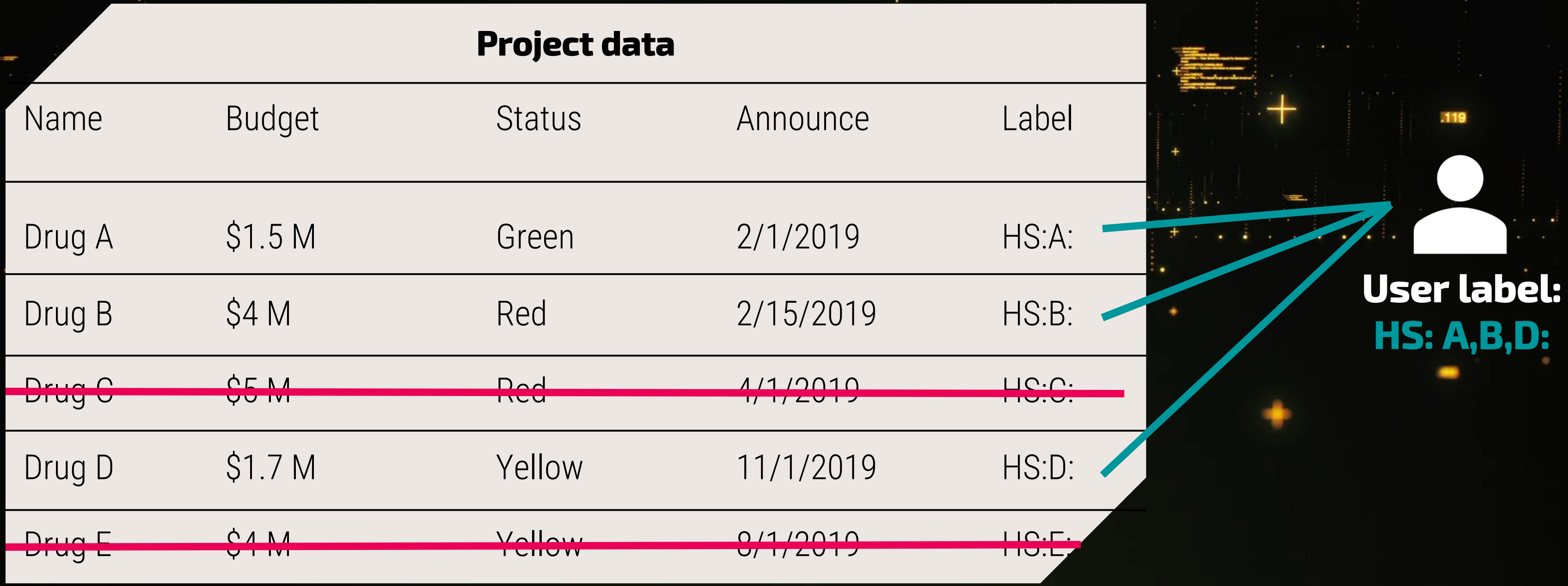
```
SQL> select Name, Budget, Status, Announce from projects
```

Project data

Name	Budget	Status	Announce	Label
Drug A	$1.5 M	Green	2/1/2019	HS:A:
Drug B	$4 M	Red	2/15/2019	HS:B:
Drug C	$5 M	Red	4/1/2019	HS:C:
Drug D	$1.7 M	Yellow	11/1/2019	HS:D:
Drug E	$4 M	Yellow	8/1/2019	HS:E:

EXAMPLE 3

```
SQL> select Name, Budget, Status, Announce from projects
```



Project data

Name	Budget	Status	Announce	Label
Drug A	$1.5 M	Green	2/1/2019	HS:A:
Drug B	$4 M	Red	2/15/2019	HS:B:
~~Drug C~~	~~$5 M~~	~~Red~~	~~4/1/2019~~	~~HS:C:~~
Drug D	$1.7 M	Yellow	11/1/2019	HS:D:
~~Drug E~~	~~$4 M~~	~~Yellow~~	~~8/1/2019~~	~~HS:E:~~

User label:
HS: A,B,D:

EXAMPLE 3

```
SQL> select Name, Budget, Status, Announce from projects
```

Project data

Name	Budget	Status	Announce	Label
Drug A	$1.5 M	Green	2/1/2019	HS:A:
Drug B	$4 M	Red	2/15/2019	HS:B:
Drug D	$1.7 M	Yellow	11/1/2019	HS:D:

User label:
HS: A,B,D:

OLS retrieves authorized data records only

LABEL-BASED SECURITY & ROW-LEVEL ACCESS CONTROL

04 ORACLE LABEL SECURITY

DEMONSTRATION

VI

EXAMPLE 3

Completed

05

ORACLE LABEL SECURITY

DEMONSTRATION

SUMMARY

06

DEMONSTRATION

SUMMARY

DEMONSTRATION

06 SUMMARY

☛ **Mandatory Access Control**

Multilevel Relation

Row-Level Access Control

Oracle Label Security

DEMONSTRATION

06 SUMMARY

Mandatory Access Control

👉 Multilevel Relation

Row-Level Access Control

Oracle Label Security

DEMONSTRATION

06 SUMMARY

Mandatory Access Control

Multilevel Relation

☛ **Row-Level Access Control**

Oracle Label Security

DEMONSTRATION

06 SUMMARY

Mandatory Access Control

Multilevel Relation

Row-Level Access Control

👉 Oracle Label Security

REFERENCE

https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_4003.htm

https://www.youtube.com/watch?v=h4kKQApaP1Y

https://www.youtube.com/watch?v=ESz4ts7g_zw

https://docs.oracle.com/en/database/oracle/oracle-database/21/olsag/introduction-to-oracle-label-security.html#GUID-47E86F58-4659-4B36-966A-69EF55E1E11D

https://docs.oracle.com/en/database/oracle/oracle-database/21/olsag/understanding-data-labels-and-user-labels.html#GUID-F29D48CE-EE9A-495E-A35B-55B38BAB1FDB

https://docs.oracle.com/en/database/oracle/oracle-database/21/olsag/access-controls-and-privileges.html#GUID-A222EB99-83C4-4BCC-84F6-D20087101E9D

https://www.tranvanbinh.vn/2020/01/huong-dan-su-dung-cong-cu-oracle-sql.html

https://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/279315.htm

https://www.youtube.com/watch?v=o4-XpUQWfaM

THANK FOR LISTENING

AND HAVE
A CUP OF TEA
^^