CS5322 Database Security

Last Lecture

- Mandatory Access Control
  - a system-wide policy decides who is allowed to have access; individual user cannot alter the policy
- Multilevel Security:
  - Each object or subject has a label
  - Whether or not a subject can access an object is decided based on their labels
  - Each label consists of two components:
    - A security level, e.g., unclassified, confidential, secret, top secret
    - A set of compartments, e.g., Asia, finance

Applying MLS to Databases

- Idea:
  - Attach a label to each database object and subject
  - Conduct access controls based on the labels
- Possible granularities of access control:
  - One label for each table
  - One label for each tuple
    - This is a common choice in commercial databases
  - One label for each value in a tuple
    - This leads to polyinstantiation

Polyinstantiation

- Idea: Use the original primary key + TC as the new primary key
- Example below: (Name, TC) as the new primary key
- As such, we may have different instances of the same tuple for different security levels
- This works, but will make things a lot more "interesting"

Name	C1	Gender	C2	Grade	C3	TC
Alice	U	Female	U	90	U	U
Bob	U	Male	U	80	U	U
Cath	U	Female	C	70	C	C
Dave	C	Male	C	60	S	S
Dave	U	Male	U	100	U	U

Coming Next

- Oracle Label Security

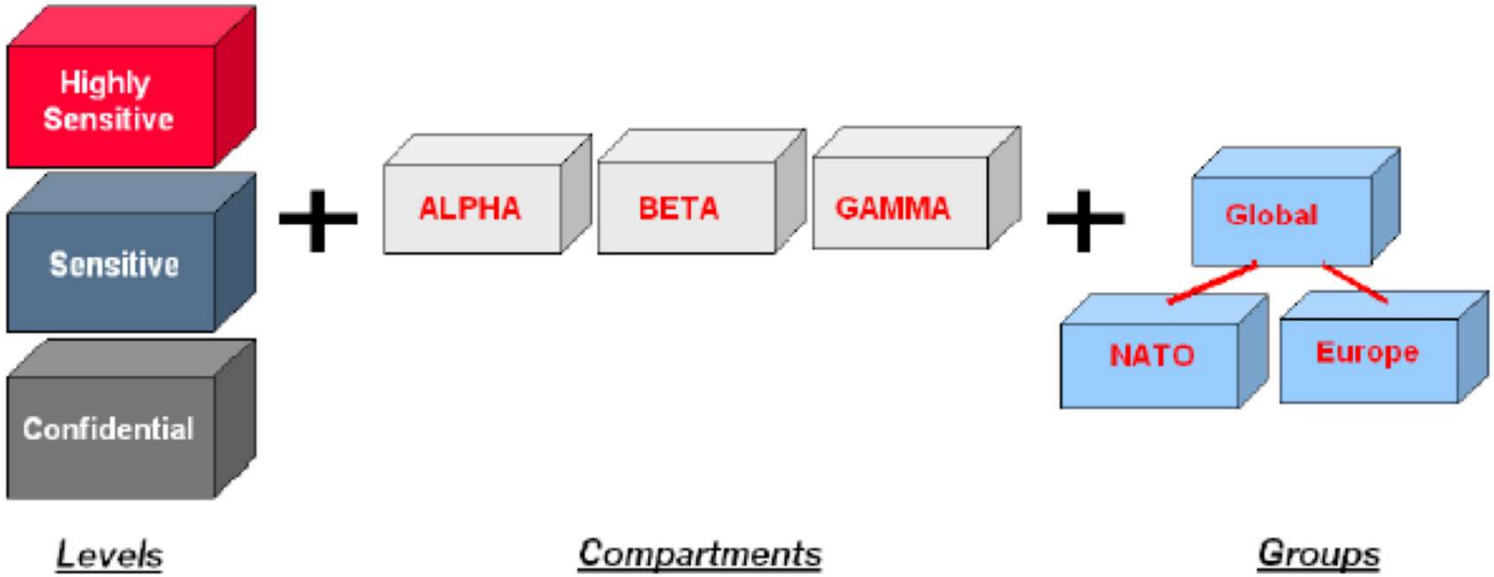
Oracle Label Security

- Oracle's version of multilevel security
- Granularity: one label per tuple
  - No polyinstantiation
- Controls access to data based on three factors
  - The label of the tuple to which access is requested
  - The label of the user session requesting access
  - The policy privileges for the user session

to help bypass their current access

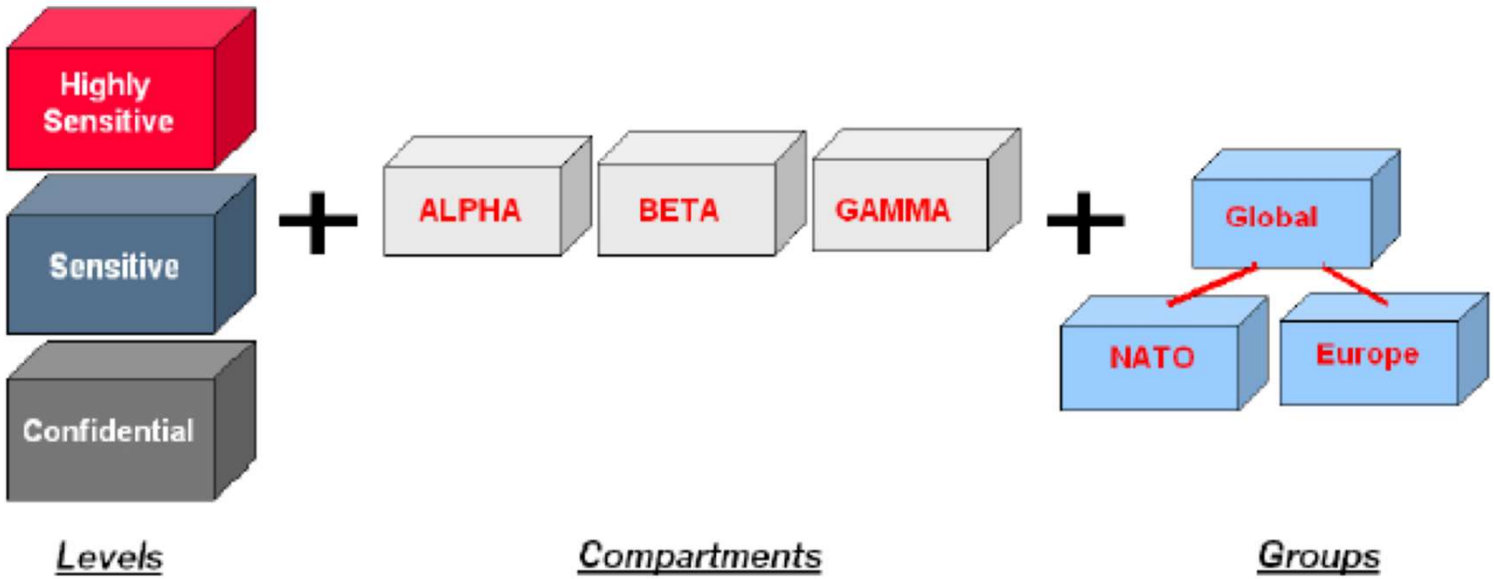
Data Labels

- Every data label has three components:
  - A sensitivity level
  - Zero or more compartments (i.e., categories)
  - Zero or more hierarchical groups



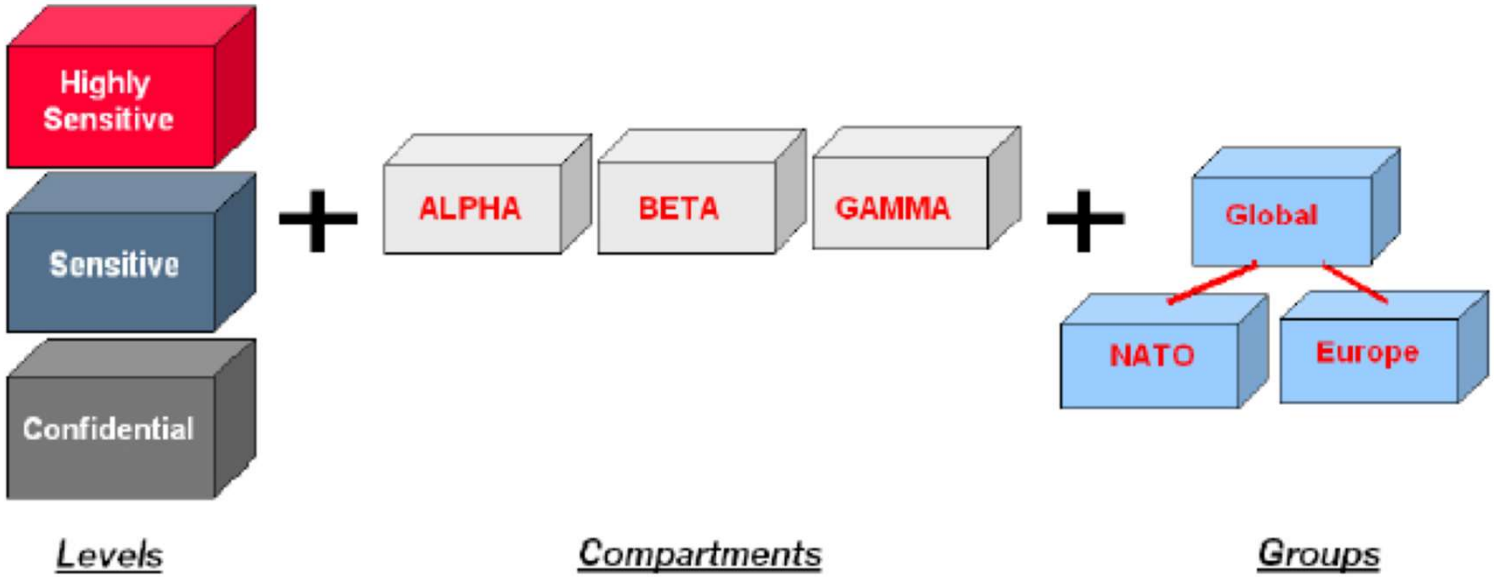
Data Labels

- Groups describe the hierarchy of ownerships
  - E.g., DCS and DISA are children of SoC, while SoC belongs to NUS
  - By the hierarchy, a user who has access to NUS data would have access to SoC data and DCS data
- Compartments describe the *areas* of the sensitive data
  - E.g., finance, chemical, international affairs



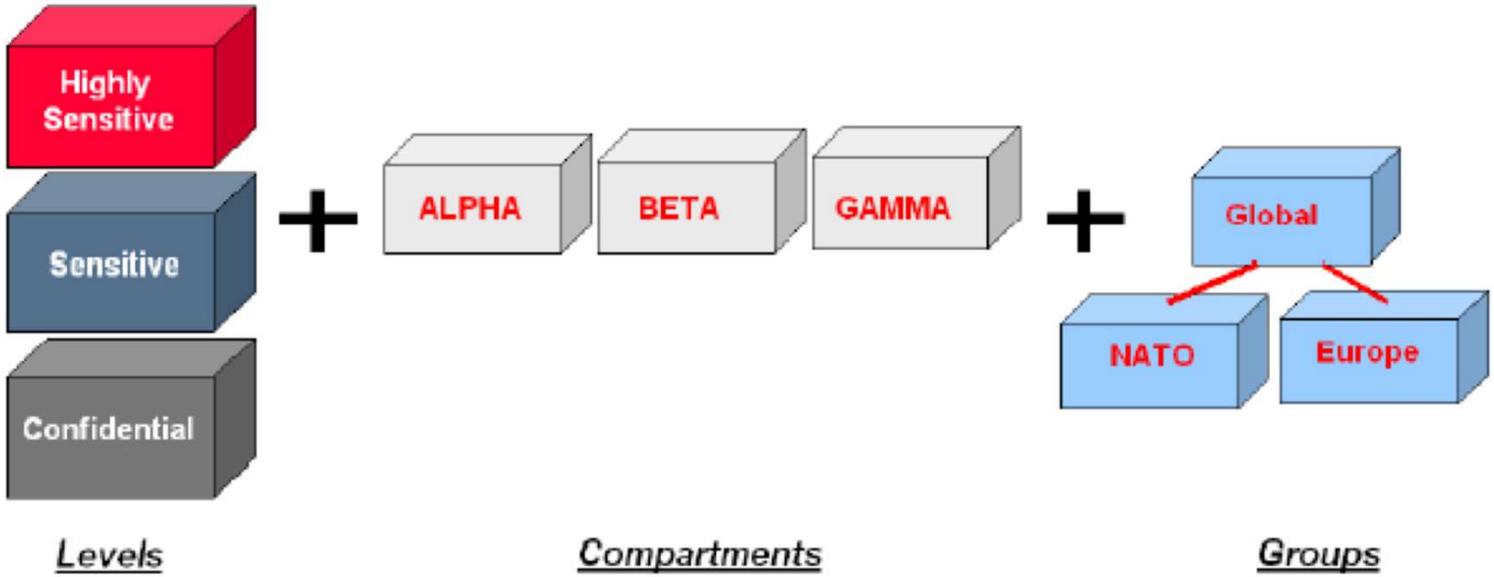
Data Labels

- Differences between compartments and groups
  - Compartments are non-hierarchical, whereas groups are hierarchical
  - If a user wants to access an tuple, she has to have access rights on **all** compartments of the tuple, but only need to have access rights on **one of** the tuple's group or its ancestor groups



Data Labels

- Each level has a character form and a numeric form, e.g.,
  - Highly sensitive (30)
  - Sensitive (20)
  - Confidential (10)
- A larger number indicates a higher level of sensitivity



Data Labels

- A label must have a level, but may or may not have a compartment or group
- So there are four possibilities:
  - A level, without any compartment or group
  - A level and a set of compartments, without any group
  - A level and a set of groups, without any compartment
  - A level, a set of groups, and a set of compartments

User Labels

- Apart from data labels, OLS also have user labels

User Labels

sacrificing the rigour of a more secure model in theory for more practical and flexible implementation

- A user label has the following components
  - Maximum level, minimum level: the maximum and minimum sensitivity level that the user is authorized to access
  - Default level: the level used by default when a user connects to the database
  - Row level: the default level for each tuple inserted by the user
  - Read compartments, write compartments: the compartments that the user is authorized for read and write, respectively
  - Read groups, write groups: the groups that the user is authorized for read and write, respectively

Access Control based on Labels

- A user session can read a tuple if all of the following conditions are satisfied
  - User's level is higher than or equal to the tuple's level
  - User's read compartments cover all of the tuple's compartments
  - One of user's read groups appears in the tuple's groups, or is the ancestor of one of the tuple's groups

Access Control based on Labels

- A user session can write a tuple if all of the following conditions are satisfied
  - The tuple’s level is higher than or equal to the user's minimum level
  - The tuple's level is lower than or equal to the user's session level
  - User’s write compartments cover all of the tuple’s compartments
  - One of user’s write groups appears in the tuple’s groups, or is the ancestor of one of the tuple’s groups

Basic Steps for Policy Creation and Enforcement in OLS

- Create a policy
- Create the levels, compartments, and groups
- Attach the policy to a schema or a table
- Attach labels to tuples, users, etc.

Policy Creation

- SA_SYSDBA.CREATE_POLICY(
  policy_name => 'emp_ols_pol',
  column_name => 'ols_col',
  default_options => 'READ_CONTROL, WRITE_CONTROL');

- emp_ols_pol is the name of the policy
- ols_col is the name of the column for storing data labels
- READ_CONTROL and WRITE_CONTROL specify when the policy should be enforced

Policy Enforcement Options

- READ_CONTROL
  - Enforce policy on SELECT operations based on the read access controls
- INSERT_CONTROL
  - Enforce policy on INSERT operations based on the write access controls
- UPDATE_CONTROL
  - Enforce policy on UPDATE operations based on the write access controls
- DELETE_CONTROL
  - Enforce policy on DELETE operations based on the write access controls
- WRITE_CONTROL
  - Enforce policy on INSERT, UDPATE, and DELETE operations based on the write access controls
- ALL_CONTROL
  - Enforce policy on all operations
- And some others

Applying OLS Polices

- A policy can be applied on a table, or an entire schema
- For different tables, the policy enforcement option could be different
- Details omitted

Privileges in Oracle Label Security Policies

potential illegal information flow

- For privileged users, Oracle Label Security can provide special privileges that allow them to bypass certain parts of the policy
- READ
  - A user with READ privilege can read all data, but is still restricted by write access controls for INSERT, UPDATE, and DELTE
  - Useful for
    - System administrators who need to export data but is not allowed to change data
    - Auditors who need to compile information from the database and generate reports, but is not allowed to change data
- FULL: can read and write all data

Privileges in Oracle Label Security Policies

- There are three special privileges for modifying the labels of tuples: WRITEUP, WRITEDOWN, WRITEACROSS
- WRITEUP
  - This allows the user to raise the level of a tuple, without compromising the compartments or groups
  - The user may raise the level up to any level at or below her maximum authorized level

Privileges in Oracle Label Security Policies

- There are three special privileges for modifying the labels of tuples: WRITEUP, WRITEDOWN, WRITEACROSS
- WRITEDOWN
  - This allows the user to lower the level of a tuple, without compromising the compartments or groups
  - The user can lower the level down to any level at or above her minimum authorized level

Privileges in Oracle Label Security Policies

- There are three special privileges for modifying the labels of tuples: WRITEUP, WRITEDOWN, WRITEACROSS
- WRITEACROSS
  - This allows the user to modify the compartments and groups of data, without altering its sensitivity level