Triggers, security and authorization in SQL

Trigger

- Statement that the system executes auto. As a side effect of a modification to the database.
- Requirements :
  - When a trigger is executed.
  - What action is performed.
- When phase is broken up into
  - Event – event that causes the trigger to checked.
  - Condition – that must be satisfied for trigger to proceed.
- Called as event-condition-action model.

- Database stores triggers just as regular data.
- Why? So they are persistent and accessible to all database operations.

Need for Trigger

- Alert humans or for starting tasks automatically when a certain conditions are met.
- Example: bank with overdraft and warehouse with items in stock.
- Trigger can’t usually perform updates outside the database.

Triggers in SQL

- Not standard before SQL:1999.
- Database system implemented in its own syntax → leading to incompatibilities.
- Triggering event can take many forms
  - Insert or delete instead of update
  - Update -> can specify which column whose update cause the trigger.
  - “Referencing old row as” used to save old value on updated row.
  - Can be triggered before event.

Security Violation

- Malicious access
  - Unauthorized reading of data.
  - Unauthorized modification of data.
  - Unauthorized destruction of data.
- Database security -> protection from malicious access. Absolute protection is impossible however.
- Security measures
  - Database Systems: users capable on accessing only portions of the database.

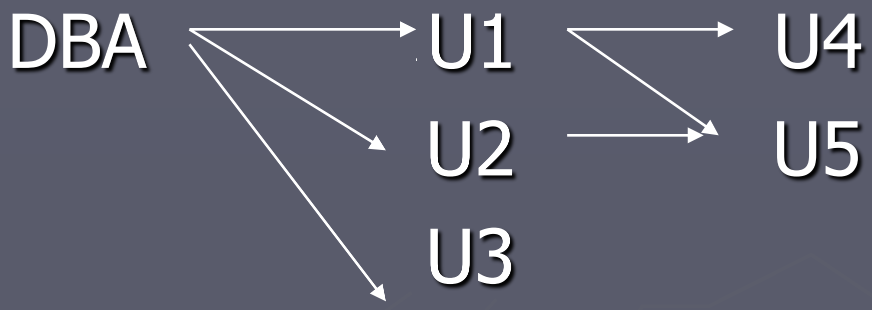
- Operating System
- Network
- Physical
- Human

Authorization

- Allow users to some of the functions of database
  - Read Autho.
  - Insert Autho.
  - Update Autho.
  - Index Autho.
  - Insert Autho.
  - etc
- Can be assigned to one or combinations of the above functions/authorization.

Authorization and Views and Priviledge Granting

- View can hide data that the user does not need to see.
  - Simplify usage.
  - Security purpose.
- User can pass on this authorization to other users (but can be revoked).
- Represented by authorization graph.



DBA

U1

U2

U3

U4

U5

This graph means that U4 is given authorization only by U1, and U5 got the authorization from both U1 and U2. If authorization is revoked for U1, U4 will lose it too, but U5 will not.

Audit trail

- Audit Trail: a log of all changes (inserts/deletes/updates) to database with information such as who did the update and when the update is performed.
- Aid security.

Authorization in SQL

- Privilege in SQL includes delete, insert, select, and update.
- Also has reference -> permits user/role to declare foreign keys when creating relations.
- How to do it?
- Grant <privilege list> on <relation/view name> to <user/role list>
- Example grant update(amount) on loan to U1,U2
- All privileges -> shortcut in giving all access.

- Usage -> authorizes user to use specified domain.
- Public -> all current and future users.
- To create roles in SQL type create role <role name>
- To grant another users/roles privilege, we append with grant option at the end of the grant statement.
- Example: grant select on brach to U1 with grant option
- To revoke, use revoke <privilege list> on <relation/view name> from <user/role list> [restrict/cascade]

- Example revoke select on branch from U1
- This behaviour is called cascading of the revoke (because other users given privilege by that user is also revoked).
- Restrict option will give error if there are any cascading.