Security in Databases

November 14, 2023

Issues

- Legal and Ethical Issues
- Policy Issues
- System Issues - levels at which security should be enforced.
- Security Levels

- DBMS typically includes security and an authorisation systems.
- Areas of consideration:
  - Preventing unauthorised access
  - Access systems
    1. discretionary
    2. mandatory
  - Statistical database security.

The database administrator (DBA) has access to a number of commands for granting and revoking access for users and groups. These include:

- account creation
- privilege granting
- privilege revocation
- security level assignment

Access Protection

- All users have a user name and password.
- Keep track of all operations (particularly updates)
- expand system log.

Operations against the database may be controlled.
Two levels of assigning privileges:

- account level
- relation level

Account level

Capabilities provided for the account:
These include CREATE SCHEMA, CREATE VIEW, ALTER, DROP, MODIFY, SELECT

Access rights provided for a relation

- follows the access matrix model
- rows correspond to subjects
- columns correspond to objects
- *Mi*, *j* corresponds to the privilege subject *i* has on object *j*
- Privilege $\in$ {read, write, update}

Can be extended in SQL to allow the following privileges:

- SELECT
- MODIFY (UPDATE, DELETE, INSERT)
- REFERENCES (can refer to relation R, when specifying referential integrity)

- Can specify privileges using VIEWS.
- Create a view over a base relation (or set of).
- Define privileges on R.

Propagation of Privileges

One can grant privileges with the GRANT option.

```
GRANT SELECT
ON EMPLOYEE
TO user22
WITH GRANT OPTION
```

Limiting Propagation

One can grant privileges with the GRANT option.
Techniques exist based on horizontal and vertical limits.

- Horizontal: can grant to at most i users
- Vertical: limits ‘depth’ of granting grants. Vertical limit zero is equivalent to granting privilege without the grant option.

- Allows a number of security classes (e.g. TOP SECRET, SECRET, CLASSIFIED, UNCLASSIFIED)
- Can be used with discretionary access control.
- Can have a number of security classes that form a lattice.
- Classify subjects as belonging to a class.
- Classify objects as belonging to a class.

Two restrictions/Properties (Bell-LaPadula Model

- A subject S is not allowed read access to an object O unless: $class(S) \geq class(O)$ (simple security property)
- A subject S is not allowed to write to an object O unless: $class(S) \leq class(O)$ (star property)

In order to incorporate multi-level security notions, we can associate classification attributes with every attribute.

- The schema then becomes

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

where TC is the classification of the tuple, set to be $max(C_1, ..., C_N)$

Apparent Key

The apparent key is the set of attributes that would ordinarily form the key.

- store entire tuple at a high classification and produce lower-level classications through 'filtering'
- polyinstantiation: multiple copies of the same tuple. Also requires modified definitions with respect to integrity rules.

Statistical Databases

- Used to produce statistics on various ‘populations’
- Individual tuples are classified.
- Queries involve applying statistical functions to a population of tuples.
- Only allow: COUNT, SUM, MIN, MAX, AVERAGE. STANDARD DEVIATION.
- Still potential may exist for ‘inference’ of classified data.

- Q1: SELECT COUNT(*) FROM <relation> WHERE <condition>
- Q2: SELECT AVG(<attribute> FROM <relation> WHERE <condition>

By modifying <condition>, we can infer data.

Can use this idea to create ‘linear set of equations’:

- `Query 1 = cond1 AND cond2 AND cond3`
- `Query 2 = cond2 AND cond3`
- `Query 3 = cond1 AND cond3`

Prevention Techniques

- Apply to query - track user queries and disallow query in the sequence that infers data. Very difficult to do.
- Apply to data
  - Suppression
  - Concealment/Disguise