BITS Pilani
Hyderabad Campus

Database Design & Applications

Dr.R.Gururaj
CS&IS Dept.

Database Security(Ch.23)

Content

- ✓ *Introduction to Database Security*
- ✓ *Threats*
- ✓*Control Measures*
- ✓*DB Security and DBA*
- ✓*Discretionary AC*
- ✓*Mandatory AC*
- ✓*Statistical DB Security*
- ✓*Flow Control*
- ✓*Encryption, Privacy*
- ✓*Challenges*

Introduction to Database Security

Database Security is a broader area that addresses many issues, including the following.

- ✓ Legal and ethical issues regarding the right to access certain information.
- ✓ Policy issues at the governmental, institutional or corporate level as what kind of information should not be made publicly available.
- ✓ System-related issues – whether the security function should be handled at the physical hardware level, the operating system, or the DBMS level.
- ✓ The need in some organizations to identify multiple security levels and to categorize the data and users based on these classifications.

Threats to databases

Threats to databases result in the loss or degradation of some or all of the following commonly accepted security goals.

- ✓ Loss of integrity- database should be protected from improper modification.
- ✓ Loss of availability- Making database objects available to users or programs to which they have a legitimate right.
- ✓ Loss of confidentiality- protection of data from unauthorized disclosure.

It is customary to refer to two types of security mechanisms:

- ✓ Discretionary Security mechanisms- Used to grant privileges to users, including capability to access specific data files, records, or fields in specific mode (read, insert, delete, or update).

- ✓ Mandatory Security mechanisms- Used to enforce multilevel security by classifying the data and users into various security classes or levels, and the implementing the appropriate security policy of the organization.

Ex: permit users to see only the data items classified at the user's own classified level (or lower). An extension to this is a role-based security which enforces policies based on roles.

Control measures

There are four main control measures that are used to provide security of data in database..

- ✓ Access control Restriction to database system as a whole. This can be done by creating user accounts.

- ✓ Inference control Statistical databases should provide only summary of the data without permitting the user to access individual data. Sometimes it is possible to deduce information by carefully querying the summary data.

- ✓ Flow control Prevents the information from flowing in such a way that it reaches unauthorized users. Such channels which violate security policies are called *covert channels*.

- ✓ Data encryption used to protect data when it is being transmitted on some communication network.

Database Security and the DBA

The *Database Administrator* (DBA) is the central authority for managing the database.
He is responsible for – classifying the users and data, granting and revoking the permissions, in accordance with the policy of the organization.
The DBA account is the super account.

The DBA privileged commands permit him to perform the following:

- *Account creation*
- *Privilege granting*
- *Privilege revocation*
- *Security level assignment*

Discretionary Access Control

The typical method of enforcing discretionary access control in database system is based on the granting and revoking of privileges.

There are two levels for assigning privileges

- *The account level* specifying privileges to accounts.
  CREATE SCHEMA, CREATE TABLE, CREATE VIEW, ALTER, MODIFY, SELECT etc.

- *The relation level* controlling privileges to access specific tables.

select privilege on R; modify privilege on R, reference privilege on R.

Grant SELECT on V to B;
Revoke SELECT on EMP From A;

Propagation of privileges using GRANT OPTION

GRANT CREATETAB to A1;

CREATE SCHEMA COMPANY AUTHORIZATION A1;

Suppose if A1 creates a table T1, he is the owner of T1 and can grant permissions to others.

GRANT INSERT, DELETE ON T1 to A2;

GRANT SELECT ON T1 to A3 WITH GRANT OPTION;
// Now A3 can grant SELECT privilege to others.

REVOKE SELECT ON T1 FROM A3;

GRANT UPDATE on EMP(Sal) TO A2; //A1 can do this

Mandatory Access Control

In many applications, an additional security policy is needed that classifies data and users based on security classes this approach is known as mandatory access control.

Typical of security classes

- *Top secret (TS) - Highest*
- *Secret(S)*
- *Confidential (C)*
- *Unclassified (U) - lowest*

In one common model (Bell-LaPadula), we have –
Subject (user, account, program)
Object (relation, tuple, column, view, operation)

According to this,

1. *A subject S is not allowed read access to an object O unless class(S) ≥ class (O), this is known as simple security property.*

2. *A subject S is not allowed to write an object O unless class(S) ≤ class(O). This is known as the star property.*

Role-based Access Control

This has emerged as a proven technique for enforcing the security in large-scale enterprise-wide systems.
Users are assigned to appropriate roles, and permissions are assigned with roles.
Roles can be created or destroyed by CREATE ROLE and DESTROY ROLE commands.

GRANT and REVOKE commands can be used to assign/revoke privileges to roles.

RBAC appears to be a viable alternative to discretionary and mandatory access controls.

Role hierarchy is a natural way to organize roles to reflect the organizations line of authority and responsibility.
Another possibility is to consider the temporal constraints that may exist on roles.

Access Control Policy for E-Commerce and the web.

Electronic Commerce (E-Commerce) environments are characterized by any transactions that are done electronically.
They require elaborate access control policies that go beyond traditional DBMSs.

The access control mechanism must be flexible enough to support a wide spectrum of heterogeneous objects.

Another requirement is support for content-based access control.

The content-based access control allows one to express access control policies that make the protection object content into account. To achieve this, the access control policies must allow inclusion of conditions on the object content.
Next, requirement is related to heterogeneity of subjects, which require access control policies based on user characteristics and qualifications.
Considering user profile while defining access policy is one solution.

Statistical Database Security

Statistical databases are used mainly to produce statistics about various populations.

The database may contain confidential data about individuals, which should be protected from user access.

However users are permitted to retrieve statistical information about the populations, such as average, sum, min, max, count etc.

The statistical database security techniques must prohibit the retrieval of individual data.

This can be achieved by prohibiting queries that retrieve attribute values and allowing only queries that involve aggregate operations on the data.

Such queries are sometimes called as statistical queries.

Statistical Database Security

Sometimes it is possible to infer the values of individual tuples from a sequence of statistical queries.

Ex.

Assume that employee data is in -

EMP(eid, name, city, age, salary, qualification, dept)

If we wish find the salary of ‘Kiran’, and we know that he is 42 years age, and lives in Pune.

We can find this by following sequence of queries.

SELECT COUNT(*) FROM EMP WHERE name=‘Kiran’ and age=42;

If the result is 1.

SELECT AVG(salary) FROM EMP WHERE name=‘Kiran’ and age=42;

Will give the salary of Kiran.

Flow Control

Flow control regulates the flow of information among accessible objects.

A flow between object X and object Y occurs when a program reads from X and writes it to Y.
Flow controls check that information contained in some object does not flow explicitly or implicitly into less protected objects. Hence a user can not indirectly get data form Y which he can't get from X directly.

A flow policy specifies the channels along which information is allowed to move.
Flow control mechanisms verify that only authorized flows are executed.
A set of rules must be satisfied to ensure secure information flows.

A *covert channel* allows a transfer of information that violates the security or the policy.
It allows information to pass from higher classification level to lower classification level through improper means.

Encryption and Public key

All the methods describes so far may not be able to protect database from some threats.

What if the data falls into some nonllegitimate hands while communicating it?

In this situation, we encrypt the message under transmission.

Encryption is the means of maintaining the security in an insecure environment.

Encryption consists of applying an encryption algorithm using some specified encryption key.

The resulting data is in encrypted form, and has to be decrypted using a decryption key to recover the original data.

DES (Data Encryption Standard) system developed by US Govt., for use by general public.

National Institute of Standards(NIST) introduces the Advanced Encryption Standards(AES) and more sophisticated than DES.

Digital Signature is an example of using encryption techniques to provide authentication services in electronic commerce applications.

Like a handwritten signature, a digital signature is a means of associating mark unique to an individual with a body of text.

A digital signature consists of a string of symbols.

Challenges in Database Security

Considering the vast growth in volume and speed of threats to databases and information assets, research efforts need to be devoted to the following issues:

1. Data quality: Database community needs techniques and organizational solutions to assess and attest the quality of data.
2. Intellectual property rights: Watermarking for relational data have recently been proposed, to protect the content from unauthorized duplication and distribution, by enabling provable ownership of the content.
3. Database survivability: Database systems are expected to operate/provide services at reduced capabilities despite disruptive events such as information warfare attacks. A DBMS should prevent an attack and detect one in the event of occurrence should do the following.
   - (i) Confinement (ii) Damage assessment (iii) Reconfigure (iv) Repair (v) Fault treatment

Summary

- ✓*Introduction to Database Security*
- ✓ *Threats*
- ✓*Control Measures*
- ✓*DB Security and DBA*
- ✓*Discretionary AC*
- ✓*Mandatory AC*
- ✓*Statistical DB Security*
- ✓*Flow Control*
- ✓*Encryption, Privacy*
- ✓*Challenges*