Frequently Used Methods for Securing Databases

MARIUTA Serban
Assistant Professor Ph.D. Student, Doctoral Studies, Pitesti University, Pitesti, Romania,
mariuta_serban@yahoo.com

Abstract: *Nowadays in the communication and electronic information era the security of a database is very necessary and also a very interesting topic either for an end user or an administrator.*

There are many categories of methods for securing databases, each of them having advantages and disadvantages. As such, choosing the proper method means knowing of these advantages and disadvantages.

For securing a database there are three fundamental principles: confidentiality, integrity and availability. Along classifying data, a complete method of securing a database require: access control to database and contained objects, backup and restore plans, audits and secured network connections.

Key words: *security of data, database security, access control, authentication, authorization.*

1. Introduction

In modern society due to fast growth of information technology and Internet more and more companies keep their data in a form of digital databases, as such database systems becoming an essential component of daily life. Any person, almost daily undertaking activities which suppose an interaction with a database such as: banking transactions, any kind of reservations, looking for books in a library or a book store.

Once in every business hardcopy documents have been reduced or even eliminated, sensitive information being stored in databases, these have become a main target for hackers. Due to this fact the database security became a very important topic nowadays.

In using databases an important part had been and also has the technologies for securing data. Starting from this, all database developers made an important point on developing and improving continuously of the security technologies in order to cope with the most dangerous attacks.

This paper deals with all the matters regarding the integrity of a database and also validity and coherence of data store.

2. Database threats

Database threats are represented by:

- Infractions assisted by the computer defined by using of computers by attackers for communication or data storing, neither of these activities being illegal.

- The terms of identity theft and identity fraud are defined by any person which illegally acquire the personal data of another person and use them no matter of the purpose (usually for obtaining material advantages).

- Breaking of codes or passwords may be seen as a tentative to avoid the security of a database and having as purpose to get in the database and obtaining sensitive information, or even undertaking illegal activities into database.

Database security means to protect it against unauthorized use, alteration or destroy of data.

Database security must be assured at the following levels:

- physical level – the space where the computers are should be protected for unauthorized access,

- human level – the access authorizations are provides and a clear evidence of these are kept,

- operating system level – any problem at this level should be solved by applying of a security measure.

- database level – there are some facilities for protecting databases.

3. Confidentiality, integrity and availability of databases

Because current databases are not containing anymore information processed by a company on a daily basis, there is a focus in protecting of data. As such almost in the same time with the creation and developing of new application which allows storing of an increasing volume of information and accessing of this information by the general public (usually by web based applications), new methods of attacking are developing.

Unfortunately, if the problems regarding integrity, availability and security of the data are not solved in due time the database become vulnerable to attacks and misusing of them. Anyway this happen, these incidents being done generate financial losses or intangible losses, such as the general public lost of trust in the capacity of the company to manage of sensitive data.

On the fundament of the security of a database lays three fundamental principles:

- confidentiality – the data should not be accessed by unauthorized users,

- accuracy, integrity and authenticity – the integrity suppose the coherence and correctness of data. Authenticity is the process of checking of the data origin and is realized by using passwords and digital signatures.

- availability and restore capacity – if the information are lost by accident or not, data should be recovered not altered. Backup of database guaranty the availability of data.

Availability suppose the possibility of accessing of information and resources whenever is needed by any authorized user.

Availability of data depends of the operating time of systems and the possibility of locating of electronic messages. All the time the data should be adequate. For a better availability of the data it is recommended to ask a confirmation from the recipient of the messages.

By integrity of database it is understood the correctness of the information provided by correct detection and preventing of several errors that may appear at the inputting data. Data integrity supposes the existing of several integrity restrictions which apply to data in order to be considerate valid, and not allowing the input of aberrant data.

The integrity restrictions can refer to the structure of data for different equalities between values expressed by declaring of fields with unique values.

The integrity restrictions are also known as integrity restrictions representing the necessary conditions that must be fulfilled by the databases in order to be considered correct and coherent regarding a real and relevant activity and are defined at the projection of database. This represents a first way to check of semantic in the database.

Taking into consideration the place where the restrictions are realized, the restrictions can be classifies into two categories:

- Restrictions that must be respected only for one relation.

These can be domains restrictions and restrictions of dependency between data.

Domain restrictions are conditions that must be fulfilled by a array of values which is allowed for the relation attributes.

By integrity of domain principle, SGBD verify a value and operations which are realized on this from two points of view: syntactic and semantic.

From the perspective of domain definition, the domain restrictions does not allow recording of a value for an attribute which are not belonging to the declared domain and can not allow operations between not compatible domains.

Domain restrictions characterizes independent properties of a domain and is referring to the semantic of the elements of the respecting domain. For example, the values of the attribute 'exam_mark' should have values between zero and ten or the attribute 'age' can not be less than eighteen.

The restrictions regarding data dependency (dependency of junction type) are realized by bonds between domains.

- Restrictions between two or more relationships

Entities integrity represents restrictions of the primary keys from the base relationships, in which an attribute of the primary key can not be NULL.

Among these the most important are the restrictions realized with the help of the foreign keys, ensuring the correct association of the relationships called referential integrity restrictions.

Referential integrity ensure guaranty finding of a foreign key in the array of the values of candidate keys corresponding to the relationship, or if restriction NOT NULL didn't impose to the relationship attributes then the foreign key has the NULL value.

Usually in the systems of the database management (SGBD) there is the restriction of keeping of the referential integrity and not allowing the changing of the data: input, delete and update. In the case of exception in which the referential integrity is not implemented into the system, it should be in the application programs.

Integrity restrictions in the SQL standard are used for understanding of the data semantic from the databases through relationship schemes. It is necessary to respect all the restrictions of integrity in order to have the correct information irrespective of the database status.

Integrity restrictions in defining the data in the SQL are divided into three categories:

- restrictions for the table realization;

- restrictions for the columns;

- restrictions for tables.

In addition of syntax content of defining data there are in SQL also additional mentions such as: foreign key restrictions representing the referential integrity restriction between a foreign key from a relationship and a primary key from another relationship. This restriction requires that the value of the foreign key to be NULL or equal to the value of the primary key at which refer and the data type of the two keys be the same.

4. Methods used for data security (technologies for data classification)

Any user who projects an application into a database is provided with the ability of monitoring of different occurring events by the system of the database management. The most often events that occur are changes regarding data, but can also be procedures or functions calls. At the occurrence of such event a process of evaluation of a condition inducted by a restriction (active rule) is started. If the condition is fulfilled the action is executed.

Correction of not fulfilling the restrictions is realized by active rules.

Database administrator is responsible for soling of all problems regarding database protection and security. This has an account called system account by which he can create accounts for users or can grant or remove different privileges.

a) The users identification method

By the process of the connection to a database a user is asked for an account and a password; management system of the database check the credentials and these are correct authenticate the user. After the authentication process the user is authorized only for specific resources, this having access only to the resources for which is granted.

Two type of authorization can be granted: an authorization right for account and authorization right of relationships. Also, every relationship is granted with an owner account created in the same time with the relationship.

In SGBD systems performances, granting the rights to the users by groups, roles etc., and the control of these rights being the responsibility of database administrator.

b) Data encryption method

For protecting data against the users who are trying to read, alter or use them in other ways than through SGBD the data encryption method is used. For decryption user identification is needed.

By data encryption method an algorithm is used to disable a user to read without having the used key for block or unblock data. Encryption is used for protecting data in the network, in the systems in which the authorization is not enough for protecting data or as an extreme measure for protecting data.

c) Using of views in applications method

For providing a certain level of security it is used the views' property of not displaying all the information from database. That way is met terms of: access at the relationship level and access at the view level. There are read-only views which do not allow changes of data, allowing only the reading of the data from the database. Such views are met in public database where information can be read by all users but changes are realized only by the database administrator.

It is not advisable changes in views because these can generate changes in different parts of database which are not visible in views. If an element which is bound by another element that does not appear in the view and his connection is unique is eliminated then this element is deleted also.

d) Administration and transfer of rights method

Each user is assigned with an access right to an object or an array of objects and the database administrator keeps an evidence of these; he also define rules of transfer from one user to another.

The right of accessing the database objects can be:

- Reading right - consulting the object;

- Inserting right - adding data;

- Updating right – replacing data but deleting data it is not allowed;

- Deleting right – just at the tuplu level, not tables.

The right of the accessing at database scheme level:

- Creation right – deleting of indexes;

- The right of creation of relationships (tables);

- The right of changing at the relationship level – deleting or adding attributes in relationships;

- The right of deleting relationships.

5. Privileges and access rights granted to users in SQL

In SQL for granting access rights to users to certain database objects instruction GRANT is user and for the revocation of these rights is used the instruction REVOKE.

The syntax of the command SQL GRANT for allocating access rights or privileges is:

```
GRANT privilege_name
ON object_name
TO {user_name | PUBLIC | role_name}
[WITH GRANT OPTION]
```

Table 1: Description of sintax for the SQL GRANT command

No.	Sintax	Sintax description
1	`privilege_name`	The name of the access right or the privilege granted to the user `ALL, EXECUTE, SELECT`
2	`object_name`	The name of the database object to which the privilege is granted. For example: `TABLE, VIEW, STORED PROC, SEQUENCE`
3	`user_name`	User's name which the right or privilige is granted
4	`PUBLIC`	All users are granted access right
5	`ROLLES`	The array of privileges that can be granted
6	`WITH GRANT OPTION`	Allow one user to grant rights to anoteher users

The syntax of the `REVOKE` command for elimination of access rights or privileges to database objects is:

```
REVOKE privilege_name
ON object_name
FROM {user_name | PUBLICE | role_name}
```

Privileges define access rights granted to users for a database object. There two types of privileges:

a) System privileges - allow user to use one of the commands: `CREATE, ALTER, DROP` on database objects.

b) Object privileges - allow user to use one of the commands: `EXECUTE, SELECT, INSERT, UPDATE` and `DELETE` on database objects.

Table 2: Examples of system privileges granted by `CREATE`

No.	System privileges	Description
1	CREATE object	Allows users to create specified object in their scheme
2	CREATE ANY object	Allows users to create specified object in any scheme

These norms apply also for system privilege ALTER and DROP.

Table 3: Applying ALTER and DROP rules

No.	Object privilege	Description
1	`INSERT`	Allows users to insert rows in a table
2	`SELECT`	Allows users the selection of data from a table
3	`UPDATE`	Allows users to update data
4	`EXECUTE`	Allows users to execute a procedure or a stored function

Being quite difficult to grant privileges when there are many users, it is advisable to use roles. Roles represent an array of privileges or access rights. By defining roles access rights or privileges are either granted or revoked to uses, or this is realized automatically granting predefined privileges.

Tabel 4: Privileges granted by the system roles

No.	System rols	Privileges granted by sytem roles
1	`CONNECT`	`CREATE TABLE, CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE, CREATE SESSION`
2	`RESURSE`	`CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER.` Using of role `RESURSE` limit the access to the database objects
3	`DBA`	`ALL SYSTEM PRIVILEGES`

The syntax for role creation is:

```
CREATE ROLE role_name
[IDENTIFIED BY password];
```

It is relatively easy to grant access rights or privileges to users by a role without grant them directly to each user.

6. Conclusions

Providing the best methods and regulations for the security of a database it is not easy, but with events which include strenghten of management control an organisation can keep safe the sensitive data.

In a first phase the security of data is realised by fulfilling of the three fundamental principles: confidentiality, integrity and availability. By defining roles and granting access rights or privileges to users is realized an additional security of the database data.

It can be said that developing a database is not so difficult as to developing a secured database.

References:

- Barnes, R. (2011) Database Security and Auditing: Leading Practices, Enterprise Auditing Solutions Applications Security.
- Băjenescu, T.I. (2003) Progresele informaticii, criptografiei şi telecomunicațiilor în secolul 20, Editura Matrix Rom, Bucureşti.
- Danubianu M., 2012, Baze de date . Fundamente teoretice □i dezvoltarea aplica□iilor în FoxPro, MECT, 2003.
- Fusaru, D. (2002) Arhitectura bazelor de date. Mediul SQL, Editura Fundației România de Mâine, Bucureşti.
- Lesov, P. (2008) Database Security: A Historical Perspective, University of Minnesota, CS 8701.
- Mihai, C.I. (2010) Modele de atac, Securitatea-informa□iilor.ro, Criminalitatea informatică.ro

Available http://www.securitatea-informatiilor.ro/tipuri-de-atacuri/modele-de-atac-113.html.

- Oltean, G. (2012) Sisteme cu logică nuan□ată, note curs,

Available http://www.bel.utcluj.ro/dce/didactic/sln/sln.pdf.

- Patriciu, V.V.; Ene-Pietroşanu, M.; Bica, I.; Văduva, C.; Voicu, N. (2001) Securitatea comerțului electronic, Editura All, Bucureşti.
- Petrescu, M., Proprietă□i avansate în standardul SQL, note curs

http://www.bazededate.org/StandardulSQL.pdf accesat 11.03.2013

- Srikanth, Radhakrishna (2011) Database security best practices

Available http://databases.about.com/od/security/a/databaseroles.htm.

- Şerban, M., Ştefan, R.M., (2012) Security Solutions for Data at Rest, Revista Economică, 5 (63), p. 174-179

  Available http://economice.ulbsibiu.ro/revista.economica/archive.php

- http://en.wikipedia.org/wiki/Database_security.

- http://www.securitatea-informatica.ro/securitatea-informatica/pierderea-sau-furtul-datelor-confidentiale-costa-companiile/

- www. beginner-sql-tutorial.com