DATABASE SECURITY - ATTACKS AND CONTROL METHODS

Emil BURTESCU[1]

PhD, Associate Professor, Department of Accounting and Management Informatics, University of Pitesti, Pitesti, Romania

E-mail: emil.burtescu@yahoo.com, emil.burtescu@upit.ro

Abstract: *Ensuring the security of databases is a complex issue for companies. The more complex the databases are the more complex the security measures that are to be applied are. Network and Internet connections to databases may complicate things even further. Also, each and every additional internal user that would be added to user base can create further serious security problems. This pupose of this paper is to highlight and identify the main methods and facets of attack on a database, as well as ways to deflect attacks, through focusing on the delicate issue of data inference.*

Key words: *attack; control; impact; inference; security*

Like all tangible assets that have to be protected by a company, valuable information stored in its computer system database is probably the most precious of assets of the company that must be protected.

Safety measures must be an integral part of any database, right from the start, at the inception and design phase. Modern approaches employed to assure the security of databases address security and protection defenses at all levels: physical, network, host, applications and data.

It goes without saying that the first of such measures has to be applied starting at the physical level and to then progress right through, reaching the data level at the other end. Initially, companies have had a rather simplistic approach, mainly due to primitive and rudimentary nature of earlier attacks, as well as the simple nature and construction of the then prevalent networks with very limited complexity if any, and did therefore focus on assuring security at the physical level. That then involved basic measures such as limiting access to locations that only authorized personnel may have access to data.

More recently, due to the rapidly changing and increased size as well as complexity and expansion of company information systems, AAA type measures began to be used (Authentication, Autorisation, Access).

Currently the necesary security measures are far more complex. These are meant to stop the highly sophisticated attacks from external attackers, and especially, from those who may very well have access to the company's internal network.

1. Classical attacks

The focus of attacks on the company's databases are motivated by the following factors:

- Databases are the mass of information which the company works with;
- Databases can reveal private data by processing public data.

Database security is relative in the next situations:

- Theft and fraud;
- Loss of confidentiality/privacy;
- Loss of privacy;
- Loss of integrity;
- Loss of availability.

The hazards which make these things happen are due in large amount to deliberate human action. Natural type hazards or random events have an impact only on data integrity and availability.

To ensure a minimum security of the databases the following requirements must be satisfied:

- Physical integrity of databases;
- Logical integrity of databases;
- The integrity of each element which composes the database;
- Access control;
- User identification;
- Availability.

The physical and **logical integrity** of databases will require the focus of efforts for protecting the physical integrity of databases, especially the recordings against destruction. The easiest way to do that is represented by regular backups.

The integrity of each element forming the database will assume that the value of each field may be written or changed only by authorized users and only if there are correct values.

The access control is being done taking into consideration the restrictions of the database administrator. DBMS will apply the security policy of the database administrator (DBA).

This must meet the following requirements:

- **Server security**. Server security involves limiting access to data stored on the server. It is the most important option that has to be taken in consideration and planned carefully.
- **Connections to the database**. Using the ODBC will have to be followed by checking that each connection corresponds to a single user who has access to data.
- **Access control table**. The access control table is the most common form of securinga database. An appropriate use of the table access control involves a close collaboration between the administrator and the base developer.
- **Restriction tables**. Restriction tables will include lists of unsure subjects who could open set off sessios.

Secure IP addresses. Some servers may be configured to receive only queries from hosts that are in a list. Oracle servers allow blocking queries that are not related to the database.

Cancellation of the Server Account. The ability to suspend an account when guessing the password is tried after a predefined number of attempts (usually 3).

Special tools. Special programs such as Real Secure by ISS which will alert in case of intrusion attempts. Oracle has an additional set of authentication methods: Kerberos security; Virtual private databases; Role-based security; Grant-execute security; Authentication servers; Port access security.

User identification will allow at any time to be known who does anything in the system. All the operations performed by users will be stored and will form a history of access. Checking the history of all hits is sometimes hard and requires a considerable workload.

Availability will allow the required data to be available for an authorized user.

2. Attacks specific to the databases

Unlike other types of data, databases may be subject to unilateral actions, in which an unclassified user has access legitimately to public information but on which he is able to infer classified information. These types of actions are called inference.

After such actions two situations are distinguished which lead to the disclosure of secret data from public data: data aggregation and association.

Two cases of inference which often appear in databases: **data aggregation** and **data association**.

Data aggregation problem arises whenever a set of information is classified at a higher level than individual levels of involved data.

Example: Military field - Individual location of vessels is unclassified, but the overall information about the location of the entirefleet is secret. Commercial - Total sales reports of different branches of the company can be seen as less confidential than the global reports of the company.

Data association problem arises whenever two values taken together are classified at a higher level than the one of each value.

Example: The list containing the names of all employees and a list containing salaries are unclassified, and a combined list containing the names and the salaries of employees is considered classified.

A first step in countering these types of attacks is the protection of sensitive data-data that must not be made public. It is considered as being sensitive data facts that are inherently sensitive, from a sensitive source, are declared sensitive, come from a recording or an attribute which is sensitive or are not sensitive in relation with other sensitive data.

Applying one or more methods of attack, and in combination with a weak protection of databases, several sensitive data types may be displayed:

Accurate data. When the database does not implement any protection mechanism, the extracted data is exatcly the exepcted ones. Queries are simple and obvious.

Bound data. In this situation an attacker can determine the range of values which the searched value can have.

Existing data. Data are classified but which can be emphasized that the existence by a process of inserting data protection mechanisms, operation refused by the protection mechanisms of the database because the data already exist.

Negative data. After some seemingly innocent queries sensitive data can be displayed. A query will be able to display data whose existence is not known, these being sensitive.

Probable data. Their existence is highlighted by complex attacks.

The success of attacks on databases relies heavily on the skills and training of the attacker and less on the automation mechanisms of attack. They use pretty much their knowledge and statistical tools, and because in this these attacks are also called statistical attacks or statistical inference attacks.

An attacker, after he passed all levels of protection and reached the database, he will try progresively a series of attacks: **direct**, **indirect** and by **tracking**.

Direct attacks are obvious attacks and are successful only if the database does not implement any protection mechanism. The displayed results will be the ones required and expected. If this attack fails then the attacker moves to the next.

Indirect attacks are attacks that are executed when it is desired the extraction of other data than tose that are displyed. Combinations of queries are used some of them having the purpose to cheat thesecurity mechanisms.

The tracking attack is applied to the databases that have impemented a supression mechanism for the claims that have dominant results. This type of attakc is used against databases that have short answers to queries. Attacks are based on the principle to which if a direct query has as result a small number of answers, the denial of the main claim will result in zero. If the answer to a complex claim is not displayed due to the supression mechanism for claims with dominant result, then the database will be queried with a set of claims and the answer to these claims will be studied, following that from these sensitive data to be extracted. In literature, this type of attack is called Linear System Vulnerability.

3. The risk

Focusing efforts to ensure database security must be done considering firstly the impact the loss of data has on the business. The final purpose must bear in mind the assurance of confidentiality, integrity, availability and data non repudiation. If the first three objectives are already classic, the last one, the non repudiation, it is necesarry in electronic transactions for confirming authenticity.

A quantitative approach of the risk is preferable than a qualitative approach because it offers a more tangible value of the situation. Even so we will still work with subjective data, estimated after an evaluation process.

If in the case of hardware loss it will be easier to estimate the loss using the cost of replacing the component, in case of a data loss the operation is far more complex. In this case we will discuss about costs for recovery. For a quantitative approach we will start from the formula for calculating the risk:

Risk = Impact x Probability

To estimate the impact we have to ask ourselves if: data can be rebuilt or restored; how long does it take to rebuild data; it is because of a deliberate action or because of accidental causes; the lsot data have special character (military, secret service, confidential).

$\mathrm{Impact}_a = \sum_{i=1}^{n} \mathrm{Impact}_i$ where: Impact$_a$ – Total impact for asset **a**; i – impact zone, (1 to 4, **confidentiality**, **integrity**, **avalability** and **nonrepudiation**).

Calculus of impact value is exemplified in next table.

Table 1. Impact value calculus

Impact zone	Impact value (USD)	Observations
Confidentiality	5 000	Loss due to the data theft. Very difficult evaluation. It implies the cooperation of several departments.
Integrity	1 000	Loss due to data spoilage. It involves costs for checking data integrity. Complex operations.
Avalability	800	Loss due to the unavailability of data. It involves costs for restoration and availability of data. Complex operations and under pressure.
Nonrepudiation	100	Loss due to orders denial.
Total	6 900	

The probability to happen an incident on the databases must be estimated by the analysis team for the security risk. The probability of generating natural events that can disrupt the smooth functioning of databases may be provided by the organizations in the field. Another category is represented by the threats specific to every company and which are linked to the human factor. Once the risk management is mature the estimation of probability of some events to occur would be more precise. Creating diagrams of evolution of the risk would help the company to concentrate its efforts one the areas that are the most affected and enhance methods of control on these locations.

4. Control methods

The classical methods of ensuring database security, the partition of database, cards, encryption, etc. Are able mostly to accomplish their tasks. Yet these are not sufficient.

Supposing we have already implemented the security mechanisms which permit us to know who the user is, then the only thing left is that we have to see what the user does. Using appropriate mechanisms for logging and auditig operations we will be able to see what every user has done and in case of incident the user to be held responsible.

Once this is made, we can go to the phase of attack control. This will involve the implementation of a mechanism that will not permit displaying sensitive data.

The options that can be chosen for such mechanism are the following:

Suppressing the applications with sensitive results. The requests for access for database elements that have as result displaying sensitive results are rejected without any response.

Results approximation. The results of request will be approximated in such way that the attacker will not be able to determine the exact values. In the case of such request the system will be able to display results close to the real ones.

Limiting the results of a request that reveals sensitive data. Limiting the result of a request which reveals sensitive data can be done in the case in which this is 1 (one).

Combining results. Combining the results from several request will create even a greater confusion for the attacker.

All these can be embedded in a monitor type mechanism which will implement de security policy of the company. Access to data will be done according to the user's classification and data classification. There is sometimes confusion between the user and the end-user. An end-user must have access only to one or more programs that run applications. A user is defined as being that person who has access to a computer system. The end-user is actually an operator and so it should stay.

Persons who work in security field or are on the other side of the barricade agree that a security ensurance system must resist 3-5 days to fulfill its purpose.

Other security controls to ensure the security of databases include control elements that are not based on the computer. Here we include **policies**, **agreements** and **other administrative control elements** different than the ones who sustain control elements based on the computer. From this category we have:

- Security policy and emergency situations plan;
- Staff control;
- Placing the equipment in safe conditions;
- Escrow agreements;
- Mainentance agreements;
- The physical control of access.

5. Conclusions

Database security presents features that must be seriously taken into account.

The first option, for a secure database is represented by its optimal protection.

Ensuring database security must be done from outside ton inside, this involving ensuring security starting from the physical level and ending with the data level (physical, network, host, applications and data).

Databases are a favourite target for attackers because of the data these are containing and also because of their volume. Datawarehouse is the ultimate goal.

Efforts to ensure database security are considerably higher than for the other types of data. It is easier to implement an access list for a great number of files than an access list for the elements of a database.

Database security mechanisms should not irritate their users.

References

1. Burtescu, E. **Problems of Inference in Databases** in „Education, Research & Business Technologies". The Proceeding of the 9th International Conference on Economic Informatics, INFOREC Printing House, Bucharest, 2009
2. Burtescu, E. **Databse security**, in „Knowledge Management. Projects, Systems and Technologies", International Conference „Knowledge Management. Projects, Systems and Technologies", Bucharest, November 9-10, 2006, INFOREC Printing House, Bucharest, 2006
3. Hsiao, S.B. and Stemp, R. **Computer Security**, course, CS 4601, Monterey, California, 1995
4. McCarthy, L. **IT Security: Risking the Corporation**, Prentice Hall PTR, 2003
5. Proctor, P.E. and Byrnes, F.C. **The Secured Enterprise**, Prentice Hall PTR, 2002
6. * * * **Security Complete**, Second Edition, SYBEX Inc., 2002

[1] Emil BURTESCU has graduated the Polytechnics University of Bucharest, Faculty of Aerospace Engineering. He holds a PhD diploma in Economic Cybernetics and Statistics at Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest Academy of Economic Studies.