Journal of Applied Business Information Systems

http://www.jabis.ro

Metrics Model for Assessing the Security of ORACLE Databases

Liviu-Adrian Vladoiu*

* Master Student at Master in Business Information Systems, West University of Timisoara, Faculty of Economics and Business Administration, Timisoara, Romania

Abstract: *Ensuring data security within a company or an organization means to align the actual requirements of information society development. The objective of this study is to present the risks an Oracle Database may face, to identify ensuring measures for its safety and security level assessment. Risk can be defined as a threat that can exploit any weaknesses in a system or an entire organization. Risk is an event that is likely to occur, often considered a random event. To prevent the occurrence of any event affecting the security of an organization or a political system it is necessary the development of a specific policy measures. These measures are determined by metrics associated to risks. Metrics are those that make a risk ranking possible. In this study was proposed a metrics model for Oracle Database security assessment. This paper suggests using a system of parameters in order to evaluate the security level of Oracle databases. This metrics model was used for auditing the security behind a Database in charge of monitoring banking transactions. As a result, we have developed a support application that uses the metrics model in order to evaluate the security levels.*
Keywords: *Metrics, Security, Audit, Evaluation, Oracle*

1. INTRODUCTION

For each and every one of us the word "security" may mean something different, depends on how and where we use it. In IT's world, the word "security" can be translated throw a set of technical procedures and by personnel which together assure that unauthorized persons don't have access to the information and authorized personnel don't put at risk the Database and the system.
Database security is still an entirely unsolved subject. Don Burleson [1], Oracle expert, advises Oracle server administrators to be more careful with their servers (hardware), as a start in the installed Database security process. Wrong installation of the Oracle server leads to the apparition of virus and hacker breach. It's confirmed that Oracle, is almost impenetrable if it is installed and configured correctly.

At organizational level, Database security is essential, those assuring the right amount of information for the different enterprise applications. Stored data in the Database, usually, include sensitive information like: employees and/or clients' information, data about the financial status of society and other confidential data. Accuracy must be guaranteed, data integrity and authenticity, and also confidentiality need.
Databases are vulnerable at security breach because of their complexity, unsure password saving, wrong system settings or some blanks left in the security system.
Reducing vulnerability risks, an organization must apply security principles like [2]:

- Less privileges, an user should have those privileges which permits him to fulfill attributions concerning the post that he occupies in the firm;
- System defend in many security levels;
- Preventing the apparition of a breach in the security system is a good thing, but detecting them is a necessity;

- Encrypting should be used as often as possible;
- Defining security policy.

Database security should point the followed aspects:

- Users authentication;
- Controlling the access to the objects and authorized applications authentication;
- Administration procedures and policy;
- Initial configuration security;
- Back-up and recovery strategy;
- Auditing.

Database risk management [2] marks thread location for integrity and authenticity of data stored in the interest Database, vulnerability reduction appealing to appropriate security policy. The risk can be defined like a thread which can exploit the weaknesses of a Database or a system/organization. For supporting the Database risk management, preventing their apparition it's recommended to appeal for a security auditing metric model.

2. ORACLE DATABASE AUDITING

"Auditing assume monitoring and selective recording of Database users"[3].Auditing is a process used for:

- Suspicious activities investigation(for example, if an unauthorized user delete data from the tables, the security administrator should verify all the base connections and the line deleting operations from the Database tables to identify him);
- Monitoring and grouping data in specific activity category in the Database(for example, Database administrator should collect statistics about modified tables, number of executed operations I/O, average session duration, used privileges, number of users that are connected simultaneous at different time intervals etc.)

The control of undertaken actions over the elements of a Database it's realized by AUDIT order, and the results of verifying are recorded in a table (AUD$) of data dictionary, known under audit trail.

Oracle system supports three general types of audit, at order level, privilege or scheme object [4]. Audit operations can be defined at session or access level.

At order level, audit refers to selective verifications over SQL commends, which can be found in the following categories:

- Orders which refer to a certain object of the scheme(for example, AUDIT TABLE checks all the commands CREATE and DROP TABLE);
- Orders which refer to certain objects of the scheme, but without specifying their name (for example, AUDIT SELECT TABLE controls all the operations SELECT over the tables and visualizations).

Audit at scheme object level consists in specific commands verification and the commands GRAND or REVOKE for the scheme objects.

Audit options at order level or privileges allow monitoring to be realized for a certain user or for a group of users. Utilizing the audit operation on a group of users may reduce the number of registrations in the AUD$ table.

3. EVOLUTION METRICS OF DATABASE SECURITY

Metric is a term utilized for showing a measure based on the references and it assumes at least two terms: measure and reference. In it's proper way security metrics should show the state or security level in relation to a point of reference and what needs to be done to avoid danger.

The National Institute of Standards and Technology [5](NIST) defines metrics like being instruments conceived for facilitating decision makings and for improving performance and responsibility throw collecting, analyzing, reporting relevant data. Metrics are simply standards or measure

systems. In this case, there are security measure standards, especially for measuring the security level of an organization. Although there are some security measure standards, ideally, security metrics should be adjust and regulated to match the situation of an organization.

- A good metric system should be:
- Constantly measured, without subjective criteria;
- Cheap for collecting data, preferred automatically;
- Expressed as a number or a percentage, not with quality labels like „big", „medium", „small";
- Expressed using at least one measurement unit like „hours", „dollars";
- In a specific context, relevant for the decision factors, so that those can take measures.

A system of metrics offers trust when they can be measured in a consistent way. Different persons should be able to apply the metric model on the same set of data and obtain equivalent answers. Metrics which depend on subjective judgments of some persons are not called totally metrics.

Metrics are calculated manually and automatically. In the first case, you can insure consisted throw the documentation of the measure process in a transparent and clear way. When people understand how and why to do something, they tend to do it in a consistent way. Keeping measure questions short helps likewise.

The cycle of a metric begins by collecting rough data, their transformation by necessity, their calculation and finally result interpretation.

4. ORACLE DATABASE SECURITY EVALUATION THROW METRICS

4.1. A METRIC MODEL SUGGESTION

We defined 5 security metrics of Oracle Database:

1. Information collecting level;
2. Configuration level;
3. Definite strategy implementation level;
4. Policy implementation level for users and objects;
5. Oracle general security level.

Metrics			
A. Information collecting level = (1+2+3+4)/4			
1. The Oracle operating system and SGBD had been identified?	NO	PARTIAL	YES
2. The users which access the operating system had been identified?	NO	PARTIAL	YES
3. The users which access the Database had been identified?	NO	PARTIAL	YES
4. All the applications which access the Oracle Database had been identified?	NO	PARTIAL	YES
B. Configuration level = (1+2)/2			
1. The operating systems had configure?	NO	PARTIAL	YES
2. The Database it had been correctly installed, configured and actualized in accordance with the policy and security procedures of the Oracle Database components?	NO	PARTIAL	YES
C. Definite strategies implementation level = (1+2+3+4)/4			
1. Authentication method had been established and configured?	NO	PARTIAL	YES
2. Was named the person who will approve the accounts?	NO	PARTIAL	YES

3. Was named who will create/erase/control the accounts?	NO	PARTIAL	YES
4. It's established a standard for the username and password?	NO	PARTIAL	YES
D. Policy implementation level for users and for objects= (1+2+3+4+5)/5			
1. The Database users' profiles in accordance with their role in the organization had been defined?	NO	PARTIAL	YES
2. Had been defined all Database sensitive data and methods to protect them?	NO	PARTIAL	YES
3. The monitoring forms had been established?	NO	PARTIAL	YES
4. Back-up procedures which are utilized had been determined?	NO	PARTIAL	YES
5. Recovery procedures had been defined?	NO	PARTIAL	YES

The first 2 metrics refer to the measure in which all the information about the operating system and Database had been collected and the measure in which they are accurate configured. The values of those 2 metrics are taken automatically from the Database and from the operating system throw the created application.

The next 2 metrics refer to the measure in which it has been defined and implemented the security strategy. The values of those information's will be taken automatically from the Database.

The last metric represents the general security level of the Oracle Database, which results in follow up from the other 4 metrics.

Each of the first 4 metrics are defined by a certain number of questions, of which answers equivalents with a certain risk level:

- Yes-has the risk level 1, this being the lowest;
- Partial- risk level 2;
- No-risk level 3, this being the highest.

Those metrics are calculated as an arithmetic mean between the risk levels associated to each answer. Each one of the metrics will be attached an importance coefficient likewise:

Metric1=5, metric2=15, metric 3=30, metric4=50.

The last metric it's calculated as an weighted mean of the first 4 metrics the importance coefficient accorded to each (formula 1).

$$\text{general level of security in Oracle} = \frac{(A \times 5 + B \times 15 + C \times 30 + D \times 50)}{100} \qquad (1)$$

Applying the defined metric model in table 1 on the Database considered it will be obtained a maxim level of risk of 3 and a minimum risk level of 1. In function of those levels it had been suggested 5 diagnosing intervals, for each interval it will be given a note likewise:

- [1;1,25) – very good
- [1,25;1,50) – good
- [1,50;1,80) – acceptable
- [1,80;2,50) – sufficient
- [2,50;3] – insufficient

The metrics defined have demonstrative character, in reality each organization defines it's security objectives in function of necessities.

4.2. THE APPLICATION OF THE METRIC MODEL ON AN EVIDENCE DATABASE OF THE OPERATIONS REALISED INTO THE BANK ACCOUNTS

For the Database in figure 1 there had been defined 3 user profiles (administrators, employees, clients) in accordance with the possible role within the organization(figure 2).

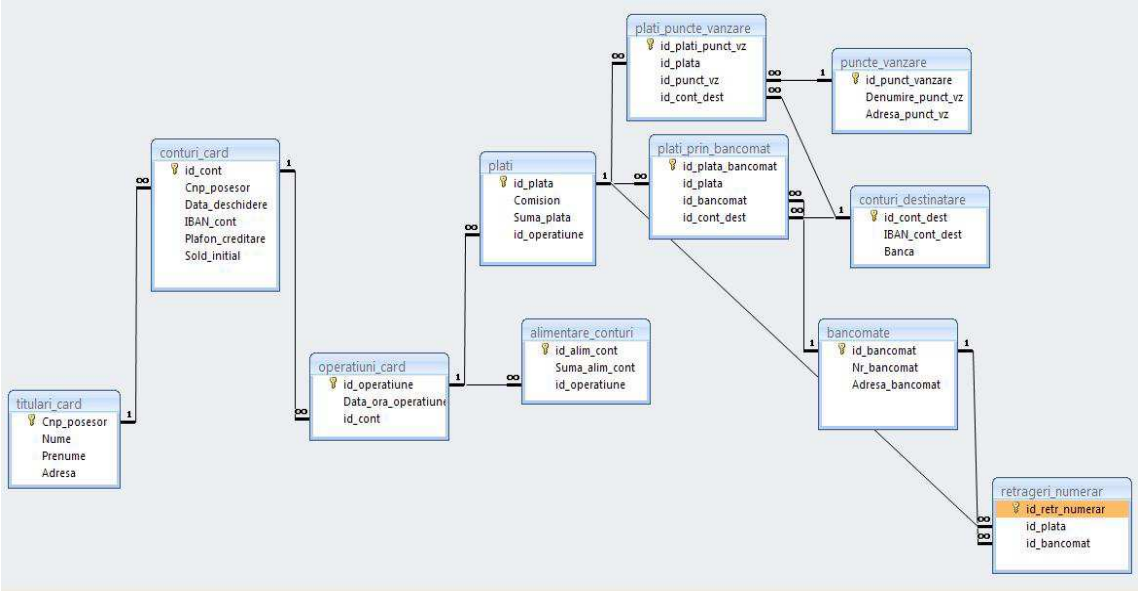

Figure 1. Database structure

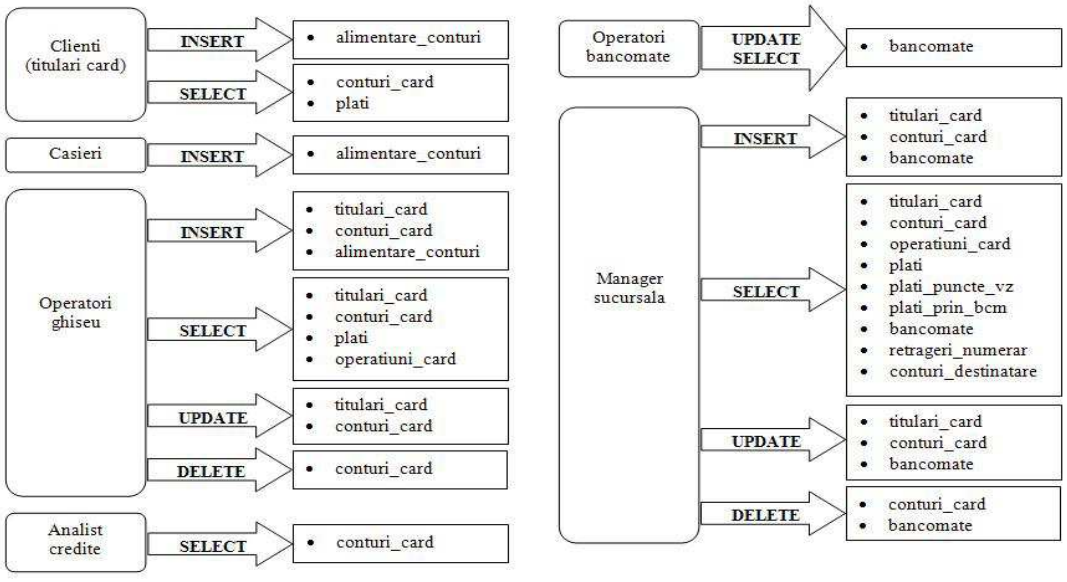

Figure 2. The role and privileges presentation

For the Oracle Database security evaluation from Figure 1 it's suggested a developed application in Delphi (Figure 3), with which the auditing of the Database security can be done (Figure 4).
The approach can be applied at the auditing of every Database.

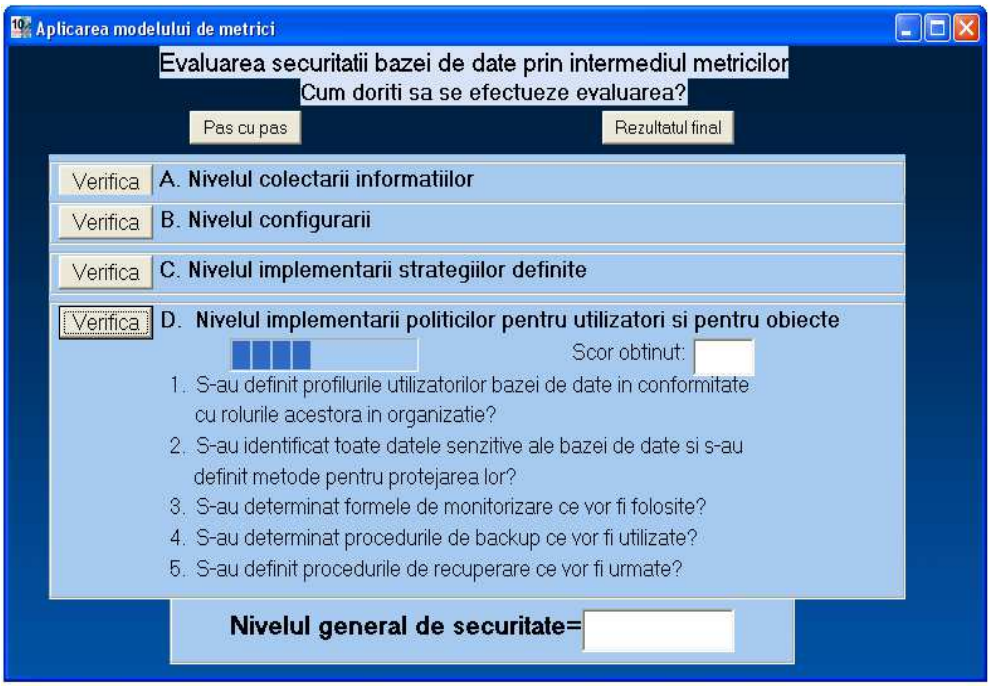

Figure 3. Application interface

Figure 4. Metric application result

5. CONCLUSIONS

Security represents a critic problem at the organization Database level. Risk factors must be eliminated so that the authenticity, integrity and accuracy of the informational context is guaranteed. Based on the principles of security, adequate considered security policy applied for Oracle Databases.
It founded a model safety evaluation metrics databases Oracle, which then applies to a particular case. The 5 metrics are calculated from the coefficients of importance given and the results are interpreted according to established diagnostic intervals.

REFERENCES

[1] http://www.dba-oracle.com/resume_don.htm

[2] Lungu Ion, Baze de date Oracle. Limbajul SQL, Ed. ASE, Bucureşti, 2005

[3] Popescu Ileana, Alecu Alexandra, Velcescu Letiţia, Florea Gabrielav - **Programare avansată în Oracle9i**, Editura Tehnică, Bucureşti, 2004, pag. 86

[4] Fotache Marin, Strîmbei Cătălin, Creţu Liviu - **Oracle 9i2: ghidul dezvoltării aplicaţiilor profesionale**, Editura Polirom, Iaşi, 2003

[5] http://www.nist.gov/index.html

[6] Fotache Marin, Strîmbei Cătălin, Creţu Liviu - **Oracle 9i2: ghidul dezvoltării aplicaţiilor profesionale,** Editura Polirom, Iaşi, 2003

[7] Fry Chris, Nystrom Martin - **Security Monitoring**, Editura O'Reilly & Associates, S.U.A., 2009

[8] Hayden Lance - **IT Security Metrics**, Editura McGraw-Hill, S.U.A., 2010

[9] Heney William, Theriault Marlene - **Oracle Security**, Editura O'Reilly & Associates, S.U.A., 1998

[10] http://download.oracle.com/docs/cd/B10501_01/server.920/a96521/privs.htm

[11] Knox C. David, Gaetjen G. Scott, Jahangir Hamza - **Applied Oracle Security: Developing Secure Databaseand Middleware Environments**, Editura McGraw-Hill, S.U.A., 2010

[12] Lungu Ion - **Baze de date Oracle. Limbajul SQL**, Editura ASE, Bucureşti, 2005

[13] Lungu Ion, Velicanu Manone, Bodea Constanţa - **Sisteme de gestiune a bazelor de date: aplicaţii Oracle**, Editura ALL Educaţional, Bucureşti, 1998

[14] Popescu Ileana, Alecu Alexandra, Velcescu Letiţia, Florea Gabriela - **Programare avansată în Oracle9i,** EdituraTehnică, Bucureşti 2004

[15] Popescu Ileana - **Oracle 8: prelucrarea avansată a informaţiei,** Editura Tehnică, Bucureşti, 1999

[16] www.infosectoday.com/Articles/Security_Metrics_Overview.htm

[17] www.isaca.org/Journal/Past-Issues/2008/Volume-5/Pages/Database-Security-Compliance-and-Audit1.aspx

[18] www.securitatea-informatica.ro/audit-securitate/evaluarea-si-managementul-riscurilor-de-securitate/

[19] www.securosis.com/projectquant/an-open-metrics-model-for-database-security-project-quant-for-databases