

Analysis of a Mandatory Access Restriction System for Oracle DBMS

This paper is devoted to the analysis of mandatory access restriction system for Oracle DBMS. As the result, several leakage channels are discovered.

For many information system based on DBMS it is often a problem to implement access restriction, which takes information value into account. It is usually crucial for large-scale information systems of government or corporate use (i.e. geographical information systems or document management systems). Such system usually imply mandatory access model. One of the features of the mandatory model is prevention of either intentional or accidental decrease of information value thanks to information flow control. Mandatory access model is implemented by labeling all the subjects and objects belonging to the access restriction system.

Oracle DBMS is currently one of the most powerful and popular industrial DBMS. Starting from Oracle9i version, Oracle Label Security (OLS) component is implemented, which makes it possible to organize mandatory access to stored data. OLS is a set of procedures and limitations built into database kernel, which allow implementation of record-level access control. In order to enable OLS it is necessary to create a security policy containing a set of labels. Whenever this policy is created it should be applied to protected tables and users should receive rights to corresponding labels.

Analysis for possible leakage channels of confidential information seems interesting for the reviewed system.

We are offering the following common analysis algorithm of the implemented mandatory access model.

- 1) Access object types are determined according to the published documentation and investigation of the DBMS (e.g., tables, strings, or columns).
- 2) Commands of SQL are analyzed in terms of how users can modify access objects.
- 3) Several objects with different confidentiality levels are created for each access object type.
- 4) Several user (access subject) accounts are created with different mandatory access rights.
- 5) A sequence of SQL-queries is formed, which are executed with different mandatory access restriction rights and objects with different confidentiality level. According to the analysis of execution of these queries it is possible to build an access model, and to make a conclusion whether the system has vulnerabilities, which can lead to leakage or corruption of confidential information.

Let us consider access objects in OLS. These are table records, which have unique labels. It is often implied that tables are access objects in OLS because security policy is applied to tables. However tables do not have labels themselves; they just contain labeled rows.

The following basic SQL operations handle individual records:

- CREATE – creation of a new record;
- SELECT – reading of an existing record;
- UPDATE – modification of an existing record;
- DELETE – deletion of a record.

Our experiments consisted of sequences of queries called by users with different mandatory access rights to objects of different confidentiality levels. These experiments made it possible to construct the mandatory access model of OLS to records. We define two variables: I and J. I is a value of object's label. Smaller values of I indicate higher confidentiality level (the value of 0 corresponds to "top secret"). J is a value of subject's access level. The model can be presented in the following formalized view:

1. CREATE \ SELECT \ UPDATE \ DELETE, $j = i$
2. SELECT, $j \geq 0, j > i$

Such mandatory access model on record-level is quite correct and it meets criteria of Bell-La Padula security model. So OLS works correctly on the level of table records.

However, beside records as representation of stored data, users can interact with other data representation, which are not affected by the mandatory access policy. Tables are an example of such objects. Users indeed can modify structure of tables, i.e. add new fields, change their names, and modify data types. OLS loses its ability to work properly on table level.

For instance, a user with higher mandatory rights has a right to create a new field in a table. The name of the field may be confidential itself, and OLS mechanism does not prevent this operation. A user with lower access rights has always a possibility to query names of all the fields.

For example, a new field is created with the name new_password_xxx (where xxx is a top secret information) with the following sql-query:

```
ALTER TABLE user1.test_table ADD (new_password VARCHAR2(30));
```

If another user who does not have any mandatory rights executes the following query (SELECT * FROM user1.test_table;), he gets an empty data set, however all field names of user1.test_table are exposed to him. As it was shown above, column name can contain classified information.

Operations shown in the example create duplex channels of data exchange between subjects with higher and lower access rights, and therefore they can cause leakage of classified information.

In the issue of the foresaid, the mandatory access model implemented in Oracle is not complete, and this fact makes it possible to exchange classified information without any control of the mandatory access system, which decreases information value.

Also you can read about actual methods of biometric keyboard signature authentication from our site:

<http://www.allmysoft.com/biometric-keyboard-signature-authentication.html>

About the Author

Original source, information about authors and contacts you can find on our page: [Analysis of a mandatory access restriction system for Oracle DBMS](#)

Source: <http://www.tntarticles.com>