DATABASE SECURITY MECHANISMS AND IMPLEMENTATIONS

Manying Qiu, Virginia State University, mqiu@vsu.edu
Steve Davis, Clemson University, davis@clemson.edu

ABSTRACT

People considering improvements in database security may benefit from this summary of security trade-offs, especially trade-offs between the level of security and the efficiency of the organization. Also this paper explains the most important database security features and describes how they have been implemented in three major commercial DBMS. The discussion covers features for protecting against unauthorized access, privileges, views, encryption, auditing, and others.

Keywords: Database, security, software

INTRODUCTION

Database security is protection of an invaluable organizational resource against unauthorized reading, changing or erasing of data. Deliberate attempts to access data without proper authority are by far the most serious security threats (3). A DBMS must have features that help enforce security measures and provide controlled, protected access to the contents of the database while preserving data integrity.

SECURITY TRADE-OFFS

There is a trade-off between the cost of reducing security risk and the adverse impact of a breech of security. There is a declining reduction in risk as the investment in security increases beyond a certain point. There is no perfect database system that will guarantee that data would never be lost or accessed by people without proper authority.

There is also a trade-off between the level of security and the efficiency of the organization (5). For example, customers who are forced to use a password having at least 15 characters and who must change their password every two weeks may decide not to use the system at all, because it is too time consuming to login and too difficult to remember the password. Here is another example. If a database system devotes too much processing time to auditing, users may find the response time too slow. Implementing extremely strong security is not always practical because of the added cost in terms of additional security software, training users, and following complex procedures. The challenge is to determine a solution that achieves the highest level of security for the least cost in both dollar value and lost user productivity.

Database developers have included features to simplify security-related procedures. A new feature of Oracle9i provides users with a single point of entry to all authorized applications with a single authentication or login process. The Microsoft SQL Server security system is integrated with the security system of the underlying Windows operating system. This makes it easier to administer the database by using the Windows user and password to authenticate access to the database as well. IBM DB2 does not require users to be defined within the database. Instead it relies on the security mechanism of the underlying operating system for performing user authentication. This turns out to be a significant advantage in scaling the database environment, especially for large organizations, since users only need to be defined once with a single password.

IMPLEMENTATION OF SECURITY FEATURES

Some analysts believe only 3 DBMS will survive the market battle: Oracle, IBM's DB2 and Microsoft's SQL Server (1). This paper focuses on how these three important commercial database systems implement security features such as protecting against unauthorized access, providing encryption, and auditing of security-related operations.

The Oracle Corporation emphasizes independently-assured secure database server products. They have worked with the sponsors of various evaluation criteria to ensure that their criteria are appropriate for layered software products such as database servers. The latest version is Oracle9i, released in June 2001. It is simply called Oracle in this paper.

IBM's DB2 targets large organizations and strives to balance providing both customers and employees flexible access to business data without compromising security standards. The latest version, DB2 Universal Database version 7.2, became available in June 2001. It is simply called DB2 in this paper.

Although Oracle9i and DB2 run on multiple platforms, Microsoft's SQL Server is restricted to Microsoft Windows. Microsoft's latest version is 8.0 (SQL Server 2000), released in January 2001 and simply called SQL Server in this paper.

Protecting Against Unauthorized Access

Oracle provides security checks based upon a list of valid users. Each user is identified by a user name and an associated password. Each user has a security domain, which is a set of properties that defines the operations the user may perform and the resource limits for the user. Each Oracle user is associated with his/her own schema having the same name as the user name. All the objects created and owned by the same user reside in the same schema. The user may grant privileges to other users to access the objects in his/her schema.

DB2 provides two levels of security checks to view or manipulate data. First, at system-level, a security program associated with DB2 does user and group authentication. It requires that the user be identified by a user name and password. Secondly, after the user has passed system-level security, the DBMS controls access to the DBMS objects and checks the permission to perform specific commands and functions. These authorizations are kept in the DB2 catalog.

A user is identified to Microsoft SQL Server by a login ID. This login ID can be created by the system administrator or can be automatically assigned from registered Windows users. In the latter case, the user can make use of a trusted connection when connecting to the database. When a trusted connection is established, the user does not need to reenter a password because

Windows has already authenticated the user. After the login IDs have been created, the system manager gives users individual access to the various databases available on the server. When a user is assigned to a database, the system manager can decide to alias the login ID to an existing user. This process is useful if a user needs to perform maintenance tasks on that database, because the user can be automatically aliased to the database owner, which gives the alias owner rights on any of the objects in that database.

Privileges

Oracle database privileges are of two types, system privileges and object privileges. The system privileges grant users power to perform the specified actions system-wide, whereas the object privileges let users perform particular actions on specified database objects—for example, to delete rows from a specific table.

Beside its system-defined roles Oracle also allows privilege grouping through user roles. A role is a named group of privileges. A role can be granted to one or more users, or can be granted to an application. Users automatically inherit all rights of all the roles they belong to. Privileges can be quickly and easily granted to a group of users by simply granting the privilege to the role. A privilege can be explicitly granted to an individual user or the user can inherit the privilege as part of a role. If the role is password-protected, the user must enter a valid password before performing an operation granted by the rights specified for the role.

In DB2, each time a user tries to use a database object, DB2 checks the user's privileges for this object. Several privilege types allow users to create and access the database resources: database, table and view, package, and index. Various authority levels provide an avenue for grouping the user privileges and higher-level maintenance and utility operations. These authorities are: system administration, database administration, system control, and system maintenance. Privileges and authorities work together to control access to the database manager and the objects in the databases.

Microsoft SQL Server allows individual users to create private objects in the database. For example if the database owner (or an alias to the database owner) has given them the CREATE TABLE privilege they can create tables. The system records the owner of every user object. Users can access objects only if the owner of the object has granted them access. An end user may be granted access to a stored procedure or view that references other objects without granting access to the objects themselves. Thus database objects can be protected from direct manipulation by adventurous end users.

Views

All the databases provide views that may be used for security purposes. A view is a way of looking at the data. Typically, it is a restricted perspective of the data in the database, which may involve looking at data from more than one table at the same time. Views help establish security by preventing direct user access to the database tables. Views can be constructed for each business application or function. Oracle9i provides row-level security, a more fine-grained alternative to views.

Encryption

In Oracle administrators can define a custom password-verification function that checks the user password against company specific rules. In addition to password encryption, Oracle provides an opportunity to encrypt other data.

A DB2 database can be configured such that during the user authentication process passwords are encrypted before being transmitted rather than flowing through the network as clear text.

SQL Server relies on encryption support that is built into the Windows operating system. It can automatically encrypt data and other network traffic as it travels between the client and server systems on a network.

Auditing

Oracle has extensive auditing facilities. Users can selectively monitor specified SQL statements, track the use of specified access rights, and record the use of specified operations on specified database objects. Audit options include whether to record successful statement executions, unsuccessful statement executions, or both. There are several predefined views to access the data recorded in the audit trail. In addition to permission settings, the auditing capabilities of Oracle allow the administrator to control almost any action performed on database objects and on the database itself. In this way any attempts to break into the database or even manipulations of data by privileged users can be logged.

DB2 has an extensive audit capability based on event monitor data. It can be customized to fulfill specific needs in an automated fashion. A user can manually create an audit-trail table to record any changes made to his/her data. The audit-trail table can be populated automatically through triggers.

SQL Server has a fully functional audit mechanism. It allows tracking usage of any permissions. A user can implement an audit trail using triggers and alerts. The alerts can be coded to send mail to an administrator when a security violation occurs.

Unique Features

Oracle allows the administrator to designate users as external or internal to control where the access privileges will be checked. The operating system checks external users. Internal users do not need an operating system account because they exist only within the DBMS.

Oracle attaches security criteria to user accounts. These criteria are automatically attached to every data access. For increased security needs, Oracle Label Security offers very fine-grained access control by comparing a tag or label attached to a data record with the label authorization profile of the current user before allowing access to the data content.

DB2's security concept takes a handshake approach with the underlying operating system and its user and group implementation. This turns out to be a great advantage in scaling the database environment, especially for large organizations, since users only need to be defined once with a single user ID and single password for them to remember. These user IDs from the operating system, as well as any grouping that may be defined, can be used for granting and revoking database privileges.

SQL Server offers flexible role-based security for server, database, and application profiles. Integrated security auditing tools can track 18 different security events and additional sub-events.

Certification

Oracle systems have been certified for the C2 level (controlled access protection: discretionary access control). In combination with hardware Oracle has been certified for the B2 level (labeled security protection: mandatory access control based on labels).

SQL Server has been evaluated by the U. S. government and has met the C2 security certification.

Stored Procedures and Triggers

Stored procedures are compiled groups of SQL statements that may be invoked by any user or application like a subroutine call. Triggers are similar, but they can automatically enforce business rules, including database security rules. Because stored procedures and triggers are compiled they generally improve performance. Also, they can simplify application programming. Stored procedures provide a way to not only to limit the privileges a user has and the data that he or she can access, but also to define a limited set of operations the user can perform within the database. Instead of using a view, a user having execute permission can run a stored procedure to update data. Stored procedures help maintain security when users log into the database directly, rather than connecting through an application, because the user can only access the information that the stored procedure allows. Stored procedures can help define privileges associated with a user's job functions and ensure data is accessed according to well-defined business rules.

Among Oracle, DB2 and SQL Server the implementations of stored procedures and triggers are quite similar. Oracle's and Microsoft SQL Server's facilities are easy to use, whereas DB2's facilities require complex coding. It may be easier to set up stored procedures in SQL Server than in other databases because a programmer can create them using a graphical interface.

Stored procedures significantly improve performance in SQL Server (2). One reason that stored procedures perform so well is that, once a procedure has been run, it is retained in the procedure cache for the next time it is needed. SQL Server uses some sophisticated algorithms to decide which procedures are retained in cache, so that the least-frequently-used procedures are more likely to be discarded if processing activity outpaces the memory limitations. Also, SQL Server tends to retain procedures that take more work to compile, at the expense of procedures that can be recompiled quickly.

It could be useful to hide stored procedure code to prevent reverse engineering of commercial applications. In SQL Server one may hide this code by including the keywords WITH ENCRIPTION when the procedure is created.

CONCLUSION

Database security features in leading DBMS have evolved far beyond the rather simplistic mechanisms in SQL that were used for many years. Even with current DBMS features, security requires a large portion of the overall effort to develop a software application (4). Accordingly, many researchers are working on better security techniques and tools. The U.S. government, especially the Department of Defense, invests heavily in this research area. Demand for research and development is likely to increase in the near future due to the sensitive and vulnerable nature of an increasing number of e-commerce applications.

REFERENCES

1. PASS Consulting Group. (2001). IBM DB2 UDB V7.2 and Oracle9i: A Technical Comparison.
2. Reilly, M. D. and Poolet, M. (2001). SQL Server 2000: Design and T-SQL Programming, Osborne/McGraw-Hill.
3. Rennhackkamp, M. (1997). Database Security, DBMS, (10,2), 67–71.
4. Simon, A. R. (1999). Strategic Database Technology: Management for the Year 2000, San Francisco, CA: Morgan Kaufmann Publishers.
5. Theriault, M and Newman, A. (2001). Oracle Security Handbook, Osborne/McGraw-Hill.