Security and Control Issues within Relational Databases

David C. Ogbolumani, CISA, CISSP, CIA, CISM

Practice Manager – Information Security

SUNGARD® Availability Services | Keeping People and Information Connected.™

Preview of Key Points

- The Database Environment
- Top Database Threats
- Key Control Layers
- Security Features within Databases
- Applications Systems and Databases
- Common Database Issues

The Database Environment

Database servers are the most important systems in virtually all organizations. They store critical information that supports business including the following:

- Email
- Financial Data
- Sales Data
- Personnel Data
- Intellectual Property
- Operation and Security Data, etc.

Modern Databases are created using Structured Query Language (SQL) which is the standard for database interoperability.

Relational Database Management System

This refers to the software system that is used to create a database and they include well known products such as the following:

- Oracle
- MS SQL and MS Access
- IBM DB2 and Informix
- Teradata (NCR)
- Sybase
- Postgre SQL
- MySQL

How Relational Databases Work

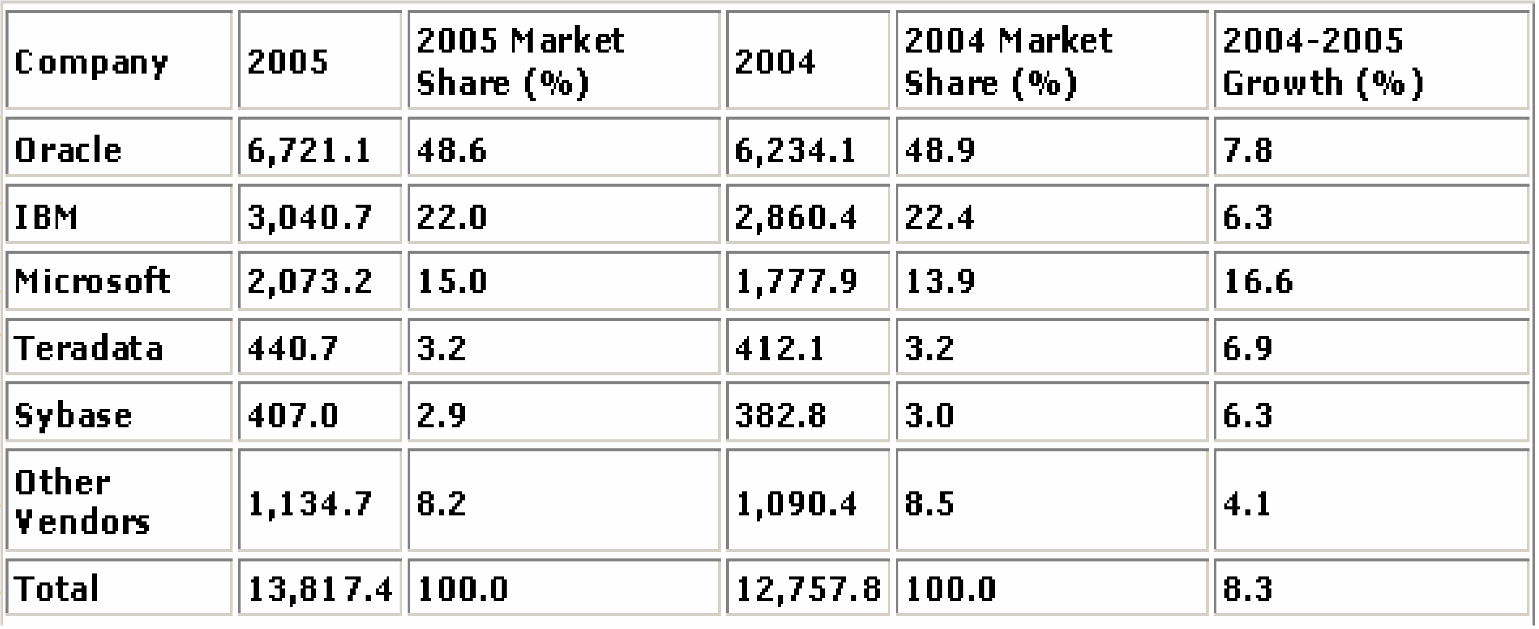
- Relational databases use a hierarchical system of tables to store information as opposed to a flat file.
- Data is organized in a structured manner using rows and columns.
- In relational databases, data is stored as “objects”.
- There are many database objects and they can be identified from views such as these:
  - Dba_objects (Oracle)
  - Sysobjects (MS SQL)

Significant Database Objects

- The more important objects that have security and controls significance include the following:
  - **Tables:** Database entity that contains rows and columns with a primary key which uniquely identifies each row.
  - **Views**: This represents data that a user can access and it is an important security mechanism
  - **Stored Procedures:** Business logic in the form of pre-compiled SQL statements that perform specific functions.
  - **Triggers:** These are typically a block of SQL statements that is executed on a table following a pre-determined event. Sometimes used for audit trails

The Current Database Market

Oracle continues to be the leader, while IBM is still a major player because of the DB2 dominance on Mainframes and AS 400.



Company	2005	2005 Market Share (%)	2004	2004 Market Share (%)	2004-2005 Growth (%)
Oracle	6,721.1	48.6	6,234.1	48.9	7.8
IBM	3,040.7	22.0	2,860.4	22.4	6.3
Microsoft	2,073.2	15.0	1,777.9	13.9	16.6
Teradata	440.7	3.2	412.1	3.2	6.9
Sybase	407.0	2.9	382.8	3.0	6.3
Other Vendors	1,134.7	8.2	1,090.4	8.5	4.1
Total	13,817.4	100.0	12,757.8	100.0	8.3

Source: Gartner Dataquest (May 2006)

Top Database Security Threats

- Privilege Abuse
  - Abusing legitimate privileges for unauthorized purposes
  - Excessive privileges that exceeds job function requirement
- Weak Authentication
  - Weak or ineffective password policies
  - Theft of login credentials, social engineering
  - Poor encryption
- Weak Systems Configuration
  - Use of default Configurations
  - Installation of improper tools and services
  - Lack of security baseline

Top Database Security Threats

- Database and Operating System Vulnerabilities
  - SQL Injections
  - Cross Site Scripting
  - Root Kits
  - Weak communication protocols
- Poor Audit Trail
- Front-End Application Vulnerabilities
- Backup
  - Incomplete and failed backups
  - Theft or improper storage of backup storage media or hard drives

Key Control Layers in Database Security

Applications as well as databases typically contain other control mechanisms which should be considered during risk assessments and audits. They include the following:

- Operating Systems
- Network Components
- Applications Systems
- Physical Security
- Database Object Security

Common Security Features in Databases

- Basic Security Mechanism in databases includes
  - Identification and Authentication requirements
  - System Privilege and Object Access Control
  - Audit Trail Mechanism
  - Data Encryption
  - Network Security
  - Auditing/Fine Grain Auditing.

Identification and Authentication

- Users can access databases through a variety of means including remotely, wireless access, scanners, through the internal network, etc. There are associated risks with each access means.
- Each user may be identified and authenticated by either the operating system or the database system. For example:
  - The Administrator can specify an Oracle password for each Oracle user when the account is created, or
  - In UNIX a user account e.g. DavidO can be Oracle user “OPS$DavidO” and connect without a password
  - This is feature disabled by default for remote users
- MSSQL has mixed authentication. Users may log in with either an operating system ID, or a separate database user account.

Reviewing Users and Passwords

- Obtain a list of all Database User Accounts
  - Describe dba_users
  - Select * from sys.dba_users
- Identify the purpose and use of each user account
  - Identify generic accounts
  - Identify shared account
  - Service Accounts
  - Guest or anonymous logins
- Review Password Policies defined in both the database and operating systems
- Check for the use of common default passwords or blank passwords.

Reviewing DB Users and Passwords

- Review user profiles as they contain the following important password control mechanism such as these settings:
  - Failed login attempts
  - Password Expiration
  - Account lockout duration
  - Minimum and Maximum password length
  - Password reuse
  - Password grace period before the account expires

- Earlier versions of SQL prior to SQL 2000 lack controls such as password complexity, expiration, lockout, and password history.

Application Systems Connections

- Popular Application Systems such as JDE, PeopleSoft, SAP/R3 and other applications also connect directly to the database
- Home grown and legacy applications also connect to the database and in many cases these are done with hard coded passwords
- Key Security and Control Issues include the following
  - Access to data outside the Application System
  - Application System Access and Security
  - Application Systems Internal Controls

Application Systems Connections

- Many popular applications as well as home grown applications are configured to use their passwords to login to the database.
- Such application may supply its UserID and password and not the end user's. In this case
  - Neither the Operating System nor Database is aware of the end user's identity
  - Neither the OS or Database (e.g. Oracle) can enforce access control decisions or monitoring based on end user identity
  - Such passwords are sometimes hard coded in the application or script and rarely changed
  - The password may be stored in a user-accessible or unencrypted file

Bypassing Application Controls

- This can occur when a user has an ID with direct access to the database and the underlying tables.
  - They can update compensation tables or other sensitive data
  - SOL*PLUS would allow the user update access outside the application
  - Risk Management professionals should evaluate database and application security to determine if level of protection is sufficient.
- Users should not be directly defined in the database if they login with a front end application.

Reviewing Access Control

- Roles, Responsibilities and Privileges
  - Rules defining what users can do
- System Privileges
  - Allows a user to perform a particular database command or operation
- Object Privileges
  - Allows a user to access an object in a particular manner
- Statement Privileges
  - selective auditing of related groups of statements regarding a particular type of database structure or schema object
- Review the operating system permissions of all key database files
- Privileges are provided directly to users or through roles.

Logging and Monitoring

- Define what actions and abuses that need to be checked such as the following:
  - Successful database access
  - Changes to database structure
  - Failed logon attempts
  - Attempts to access the database with non-existent user names
  - Attempts to access the database at unusual hours.
  - Checks for users sharing database accounts
  - Multiple access attempts using different usernames from the same terminal
- Database auditing is viewed as being complex and slow but this is generally not true.

Backup and Recovery

- Ensure that an appropriate backup and recovery strategy exists
- Oracle has a number of backup and recovery mechanism including the following
  - Redo and archive logs
  - Import and export utilities
  - Partial and Full database backup
- SQL Server has a number of back-up features including
  - Database backup
  - Transaction log
  - Differential backup
  - File / File group backups

Vulnerability Analysis

- Conduct periodic Vulnerability Assessments

- Vulnerability Assessment Tests probe for known vulnerabilities
  - Identify vulnerable software versions
  - Identify vulnerable services
  - Probes the database for known weaknesses
  - Test for default and weak passwords

- Common tools that are used for the following include
  - Nessus, Retina, Saint (Generic Assessments)
  - App Detective, NGSSquirrel, (Specific to Databases)

Common Database Security Issues

- Users with excessive privileges
  - Users with administrative privileges
  - Users whose privileges are higher than their role requires
  - Users who have moved or changed job roles
- Lack of logging and No Auditing of Privileged users
- Failure to Segregate Duties appropriately
- Inadequate review of Audit logs
- Generic, shared, and terminated users with access to production systems
- Guest user in production databases
- Improperly configured systems and weak patch management
- Incomplete backup and failure to encrypt backup data

Q&A