Global Information Assurance Certification Paper

AN OVERVIEW
OF
ORACLE DATABASE
SECURITY FEATURES

Prepared by

Lorraina Hazel, CNE
SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

May 13, 2001
An Overview

of
Oracle Database
Security Features

Introduction

The intent of this paper is to give a new user of Oracle database software, or anyone considering the use of Oracle or an Oracle application, a basic understanding of the security capabilities of Oracle database software. It is beyond the scope of this paper to cover all of the countless security features and options available in Oracle. This paper covers Oracle 8i release 3, unless otherwise noted. Although the newest version, Oracle 9i is expected to be available during the Spring of 2001, Oracle 8i is currently the most widely used. Oracle database software has many sophisticated security features which make it an excellent database system for practically any application. Data confidentiality, integrity, and availability can all be well protected with a properly designed Oracle database.

For those organizations that require a very high level of security, such as medical facilities and e-commerce sites, the more sophisticated capabilities of the Oracle Advanced Security option should be considered. This paper includes a brief description of this optional add-on product.

Authentication

Oracle allows for various types of authentication. Oracle-based authentication allows for Oracle database accounts with user-ids and strong password management (see Profiles below). Oracle passwords are encrypted with a modified DES algorithm for each database connection. Oracle passwords are stored in an encrypted format in the data dictionary.(11) Each session key is unique and is not re-used. All passwords are encrypted, including user passwords whether across the network or local connections, server to server passwords, and even database administrator passwords when the database is down.(1) Oracle also supports host-based authentication which is based on the operating system's user accounts which are then passed on to Oracle. Additional authentication options are available for those that choose the Oracle Advanced Security Option (see below).

Profiles

Oracle makes use of profiles to allow the administrator to place specific restrictions and controls on a number of system resources, password use and various Oracle products. These profiles can be defined, named, and then assigned to specific users or groups of users. There are two types of profiles, which are system resource profiles and product profiles.

System resource profiles can be used to put user limits on certain system resources such as CPU time, the number of data blocks that can be read per session or program call, the number of concurrent active sessions, idle time, and the maximum connection time for a user. Use of this option can ensure that users don't unintentionally or maliciously "hog" system resources. Additionally, system resource profiles can be used to define and enforce password rules such as password life, grace logins, and account lockout after a defined number of failed login attempts. Perhaps the most impressive feature of this type of profile is the ability to have password complexity checked against a custom password complexity function. The database administrator

can write a custom PL/SQL function to define just how complex a password must be, such as number of alpha, numeric and/or numeric characters, length, and how different a new password must be from the previous one.(3, 4)

Product profiles can be used to prevent users from accessing specific commands or all commands in Oracle SQL, SQL*Plus, SQL*ReportWriter, and PL*SQL. Use of this option allows the administrator to do such things as prevent user access to the operating system (SQL*PLUS HOST command), and to prevent unauthorized copying of data from one table to another (SQL*PLUS COPY command).(3)

Privileges

By default, new Oracle users are not given any privileges. New users must be given privileges before they can logon or execute any database operation. Users can not do anything unless they have been given the specific privilege to do so. There is an impressive number of privileges that can be given, around 100 in all. There are two types of privileges available to be granted to users. They are system and object privileges.

System privileges allow a user to create or manipulate objects, but do not give access to actual database objects. System privileges allow a user to execute commands such as ALTER TABLE, CREATE TABLE, EXECUTE ANY PROCEDURE, and DELETE TABLE.

Object privileges are used to allow access to a specific database object, such as a particular table or view. Object privileges that are given at the view level are especially impressive. This allows for an administrator to give users access to a chosen sub-set of columns or rows in a table, rather than the entire table.(1) Oracle also allows for the user of the GRANT privilege which allows a user to GRANT their privileges to another user or role (see Roles below) for objects that they own.(3, 5)

Roles

Roles are used to ease the management task of assigning a multitude of privileges to users. Roles are first created and then given sets of privileges that can be assigned to users and other roles. Users can be given multiple roles. It is much easier to create sub-sets of privileges that are organized into roles and then assign the role to one or more users. Roles can be protected with passwords. Roles that are protected with passwords require that a password be provided before activating a role unless it is the user's default role. The password feature can be useful in situations where a user needs access to data through an application but it is not desirable to give the user direct access to the data through the use of a report writing tool, etc. The password can be supplied by the application, thus preventing the user to even need to know the password.(5)

Oracle has three default roles which have certain privileges already assigned. The Connect Role is useful only for occasional users because it only allows user login and the ability to create their own tables, indexes, etc. The Resource Role is similar to the Connect Role, but allows for more advanced rights such as the creation of triggers and procedures. The Database Administrator Role is granted all system privileges needed to administer the database and users.(4)

Database Availability Features

Oracle 8i has a number of features that allow it to support mission critical applications that require reliability, continuous operation and recoverability in the event of a system failure. Some of these features are as follows: (6)

- Control users with profiles to prevent intentional or unintentional system resource "hogs".
- A number of backup options are available. "Cold" backups allow backups when the database is down. "Hot" backups allow backups to be done while the database is up. Logical backups or "exports" take a snapshot of the database at a given point in time by user or specific table(s) and allow recovery of the full database or of single tables if needed. There is also a sophisticated Recovery Manager facility which catalogs backup sets to aid in successful recovery.
- Database replication facilities can be used to create a duplicate fail-over database site in case of system failure of the primary database. A replicated database can also be useful for off-loading large processing intensive queries.
- Oracle Parallel Server makes use of two or more servers in a cluster which access a single database. A cluster can provide load balancing, can scale up more easily, and if a server in the cluster fails only a sub-set of users may be affected.
- Data partitioning can be used by administrators to aid in the management of very large tables. Large tables can be broken into smaller tables by using data partitioning. One advantage of partitioning is that data that is more frequently accessed can be partitioned and placed on faster hard drives. This helps to ensure faster access times for users.

Database Encryption

At first thought, it might seem desirable to encrypt a confidential database. However, if the proper user access controls are in place than an encrypted database would only provide protection from unauthorized users and, of course, the database administrator who has unlimited access. It must be remembered that encryption has a high cost in over-head due to the processing power needed to execute the complex encryption/decryption algorithms. For these reasons, Oracle 8i does not provide full database encryption.(1) However, Oracle 8i does provide a special PL/SQL package which can be used to encrypt and decrypt data using DES and Triple DES. This can be used to do partial database encryption.(10)

Auditing

There are three standard types of auditing available in Oracle, including SQL statement-level, privilege-level, and object-level auditing. Audit records can be written to the standard Oracle audit table, to an operating system audit trail (dependent on operating system used), or to an external file. The three basic types of auditing can be done by user, successful or non-successful attempts, and by session or access time intervals. The standard auditing is useful but is at the table level. It can not be used to audit at the record or column level.

In order to address the limitations of the standard package auditing, Oracle now has the ability to audit through custom audit programming. Oracle allows for custom audit programs through the use of database and event triggers. Database triggers are PL/SQL programs that are stored

within a table and are executed before, after, or *instead* of certain commands when they are executed. For example, this could allow for the writing of an audit record each time a change is made to a particular row in a database. Event triggers can be used to write Oracle audit messages on the events such as login, logoff, and other database events.

Through the use of the standard auditing capabilities and the custom trigger programs, it is possible to audit an endless number of possibilities such as: (3, 4, 5)

- Execution of a specific SQL statement, such as auditing table manipulation operations or user connections.
- Use of system privilege(s), there are over 90 privileges such as create view, create table, etc.
- Audit by object, to see what was done to an object (tables, views, indexes, etc.).
- Audit specific user(s).
- Audit middle tier applications, such as access by another database
- Audit successful and/or unsuccessful events.
- Audit changes to a specific row or column.
- Audit a potential change to a row and *instead* write a record to another table to await approval from a manager.

Protecting Data Integrity

Oracle provides several features to ensure data integrity whether in the case of system failure, human error, or malicious attacks. These features include redo log files, rollback segments, and LogMiner.

All data changes are recorded in at least two redo log files that are maintained by Oracle. In the event of a system failure or data corruption, the last good backup and the redo log should be restored to bring the system back to the state it was before the corruption or data loss.

Oracle uses rollback segments to record the state of the database prior to each change. In the event of a system failure or corruption event, the rollback segment can be used to back-out any uncommitted changes to restore the database to the state it was prior to the last uncompleted transaction(s).(3)

Oracle has a SQL-based log file analyzer utility called LogMiner. LogMiner can be used to analyze the redo log files and rollback segments when a more sophisticated restoration process is required.(6)

Oracle Advanced Security Option

The Oracle Advanced Security Option (OAS) includes features which ensure secure communications when accessing a database even over the internet. RSA RC4 (40, 56, 128, and 256 bits available) and Triple DES can be used for data encryption over a network. OAS uses the MD5 cryptographic checksum and Secure Hash Algorithm (SHA) for securing the integrity of network messages.(9, 10)

OAS offers additional authentication options. OAS allows for user and database to database authentication through the use of X.509 v.3 certificates. The database to database authentication

can be used to enforce the authentication of databases that reference each other. OAS also allows for the use of SSL, RADIUS, Kerberos and CyberSafe, Smart Cards (RADIUS-Compliant),Token Cards (SecurID or RADIUS-Compliant) , Biometric Authentication (Identix or RADIUS-Compliant) and BULL ISM.(1,2) Single sign-on is also supported with digital certificates over SSL.

OAS can be integrated with Oracle's Internet Directory. Oracle's Internet Directory is an optional LDAP compliant directory which can be used to centralize and manage users in one directory rather than in multiple databases. Use of the directory also makes single sign-on possible, thus eliminating the need for users to remember multiple passwords for various applications.

The Oracle Company's Commitment to Security

In 1990 Oracle formed a "hack team" to begin a proactive approach to finding and fixing product vulnerabilities. This team was initially formed to perform a United States government "Orange Book" evaluation of Oracle products. The team is comprised of Oracle staff and external computer security experts. This team conducts extensive security assessments on Oracle products using current hacking tools, known bugs, and their own expert knowledge of the products and computer security. Oracle's goal is to provide secure products that are secure "out of the box" using the default installation.

In addition to self-evaluation, Oracle has made a major commitment to having its products undergo extensive evaluation by a number of national and international security evaluation organizations, two of which are the US National Computer Security Center, and the International Common Criteria (CC). Oracle products have obtained more security certifications than any other database vendor.(7) For more information on Oracle security certifications, see http://www.oracle.com/ip/solve/security/seceval_wp.pdf. For information on the current status of security certification see http://technet.oracle.com/deploy/security/seceval/pdf/seceval_matrix.pdf.

Recommendations

- If considering the purchase of an Oracle application, ask the vendor about how they have incorporated Oracle security features into their product. In other words, don't assume that the application makes use of the security capabilities of Oracle.
- Be prepared to give your in-house staff the training needed to support and maintain an Oracle database application, even if using a 3rd party application.
- If considering the purchase or Oracle Advanced Security option, be sure to check on all product and application dependencies and requirements. For example, Oracle Advanced Security requires the use of Oracle 8i Enterprise Edition and not all applications support the use of Oracle Advanced Security option.
- If considering the use of Oracle as a development platform, be prepared to have the resources necessary to train your developers. Undertaking the development of an Oracle application is no small endeavor.
- Be sure to check and fix the latest Oracle vulnerabilities. Information can be found at http://technet.oracle.com/deploy/security/alerts.htm.

REERENCES

1. “Database Security In Oracle8i” An Oracle Technical White Paper, November 1999, URL: http://technet.oracle.com/deploy/security/pdf/oow99/dbswp86.pdf (13 May 2001).

2. “Untitled”, An Oracle 8i Overview, URL: http://technet.oracle.com/deploy/security/oracle8i/htdocs/overview.htm (13 May 2001).

3. Theriault, Marlene, and William Heney, Oracle Security, Sebastopol CA: O'Reilly & Associates, Inc., 1998.

4. Koch, George, and Kevin Loney, Oracle8: The Complete Reference, Berkely CA: Osborne McGraw-Hill, 1997.

5. Kreines, David C., and Brian Laskey, Oracle Database Administration, Sebastopol CA: O'Reilly & Associates, Inc., April 1999.

6. "Meeting the Availability Needs of the Mission-Critical Enterprise with Oracle8i" An Oracle Business White Paper, February 1999, URL: http://www.oracle.com/collateral/o8i_high_avail_enhance_fo.pdf (13 May 2001).

7. Smith, Howard, "Hack Proofing Oracle", Oracle Corporation UK Limited, URL: http://otn.oracle.com/deploy/security/pdf/oow00/orahack.pdf (13 May 2001).

8. "Computer Security Criteria: Security Evaluations and Assessment" An Oracle White Paper, October 2000, URL: http://www.oracle.com/ip/solve/security/seceval_wp.pdf (13 May 2001).

9. "Introduction to Oracle Advanced Security", Oracle Advanced Security Administrator's Guide, Release 8.1.5, URL: http://technet.oracle.com/doc/network.815/a67766/toc.htm (13 May 2001).

10. "Oracle 8i Release 3 New Features Summary" Features Overview, August 2000, URL: http://technet.oracle.com/products/oracle8i/pdf/8iR3_nfs.pdf (13 May 2001).

11. "Oracle 8i Concepts" Controlling Database Access, URL: http://technet.oracle.com/docs/products/oracle8i/doc_library/817_doc/server.817/a76965/c25acces.htm (13 May 2001).

*Note: Some of the above URL addresses may require the creation of a free account to login with.