Oracle9i Label Security ™ – Controlling Access to Data

An Oracle White Paper
January 2002

ORACLE

Oracle9i Label Security – Controlling Access to Data

EXECUTIVE OVERVIEW

Sensitivity labels are most commonly associated with defense weaponry designs and military operations. A new military jet fighter project might be given a special code name and project personnel might be required to have special security clearances. However, sensitivity labels are also used in commercial organizations. For example, a commercial company usually has information which is considered public, internal, confidential or highly sensitive. Oracle9i Label Security ™ links the sensitivity label with data such that administrator's can control access to data by defining user label authorizations in Oracle9i. Oracle9i Label Security incorporates concepts used in government intelligence agencies worldwide for controlling access to data. Oracle9i Label Security introduces powerful new technology which gives government and commercial organizations the ability to better manage privacy rules and access to information.

INTRODUCTION

Sensitivity labels provide powerful access control capabilities. A sensitivity label can be as simple as a company name, or it can be a complex series of code words added to a document being delivered to the President of the United States or the Chief Executive Officer of a corporation. A sensitivity label can be used to restrict access to patient medical records or to protect an ongoing criminal investigation.

PROTECTING SENSITIVE DATA

Oracle9i Label Security is designed to address the sophisticated access control requirements found in today's Internet environment. It is the first label based access control product designed specifically for the most popular commercially

available operating systems. Oracle9i Label Security enforcement options allow security policies to be finely tuned for specific industry environments.

Out-of-the-box Virtual Private Database

Oracle9i Label Security requires no software development

Oracle9i Label Security is a powerful, out-of-the-box security solution which eliminates the burden of writing and maintaining Oracle VPD FGAC PL/SQL security policies to enforce row level security. Oracle9i Label Security is built on the Oracle virtual private database (VPD) fine grained access control (FGAC) technology. VPD FGAC gives administrator's the ability to program security policies using Oracle PL/SQL and assign the security policies to database objects. Oracle9i Label Security requires no software development. Oracle9i Label Security is an ideal solution where access control is based on the sensitivity of data and traditional access control mechanisms are not sufficient.

Object Privileges and Row Level Security

The Internet is increasing the need for row level security because more information is being stored in a single location.

Database objects include the database tables which store application data. A typical database application may contain dozens or even hundreds of database tables. For example, imagine a simple order entry application which contains two database tables. The first table (*purchase orders)* tracks purchase orders. The second table (*items)* tracks specific items included in the purchase order. For each purchase order listed in the *purchase orders* table there may be one or more items in the *items* table. Access to the data in these tables is mediated using database object privileges such as SELECT, UPDATE, INSERT and DELETE. Object privileges can be granted directly to an application user or managed through enterprise roles. Roles contain the object privileges necessary to perform a specific job function. For example, the object privilege SELECT might be given to CLERK role. In most cases object privileges are sufficient to satisfy stated security policies. For example, a user can be denied access to purchase order information by simply ensuring the user does not have any object privileges on the underlying purchase order application tables.

Row level security is the ability to control access to individual rows within a database table after an application user has been given object privileges on the database table. For example, suppose a security policy states that an application must be capable of filtering out purchase orders labeled *company sensitive* ? By default, giving an application user the SELECT privilege on the *purchase orders* table will allow the user to view all information. One approach to solving this requirement is to create two database views. The first view will exclude all the purchase orders deemed *company sensitive* and the second would include all the purchase orders. This approach is problematic because the security policy may change to include new levels of sensitivity. In addition, application users will need to be assigned the correct enterprise role depending on their authorization to view company sensitive information. Sensitivity labels solve this security requirement and eliminate the need for additional views. The Internet is increasing the need for row level security because more information is being stored in a single location.

Oracle9i Label Security and Sensitivity Labels

Reduces application size and complexity and increases security

Oracle9i Label Security uses sensitivity labels to control access to data. This is sometimes referred to as label based access control (LBAC). Oracle9i Label Security does not alleviate the need to manage object privileges discussed in the previous section. Oracle9i Label Security adds security to the database which no other database vendor currently provides. Oracle9i Label Security performs an additional security check after the standard object privileges have been verified. It eliminates the need to create multiple views and manage the associated object privileges when attempting to implement row level security. It reduces application size and complexity and increases security by moving row level security into the database and out of the application logic. Incorporating sensitivity labels into the access control decision process addresses a common and complex security requirement. Oracle9i Label Security sensitivity labels contain a single sensitivity *level* , or a *level* combined with *compartments*, *groups* or both. The ability to use all three in a sensitivity label provides multidimensional row level security.

Example Sensitivity Labels:

Confidential : : Asia

Top Secret : FX-Fighter Jet : Air Force Command

Sensitive : Vaccine Trials : Center For Disease Control

Confidential : Global Warming : United Nations Security Council

Sensitivity Levels

Levels – Internal, Confidential, Sensitive, Highly Sensitive

One component of the data sensitivity label which Oracle9i Label Security supports is known as a level. The easiest way to understand levels is to use an example. The novel *The Hunt For Red October* by Tom Clancy, is based around a fictional super quiet Russian submarine. The existence of the submarine is an example of an extremely high sensitivity level, such as *Top Secret*. In this example, personnel whose authorizations do not meet or exceed the *Top Secret* authorization will be restricted from viewing details assigned to this sensitivity level.

- *Level* -- The level is a hierarchical component which denotes the sensitivity of the data. A typical government organization might define levels confidential, sensitive and highly sensitive. However, there is no requirement to define more than one level. For example, a commercial organization might define a single level for company confidential data or application hosting requirements.

Sensitivity Compartments

Compartments – Company Separation, Projects, Technology, Test Results

Another component of the data sensitivity label which Oracle9i Label Security supports is known as a compartment or category. In *The Hunt For Red October* the water propulsion system is an example of a sensitive technology which might be assigned a security compartment. In this example, personnel whose responsibilities do not include the water propulsion system can be restricted from viewing details assigned the sensitivity compartment.

- *Compartment* - The compartment component is sometimes referred to as a "category" and is non-hierarchical. Typically one or more compartments are defined to segregate data. For example, a compartment might be defined for an ongoing strategic initiative, or might map to a hosted application subscriber. Users can be given read only or read-write authorizations on an individual compartment basis, providing powerful row level security.

Sensitivity groups

Groups – Organizational ownership, finer granularity

Another component of the data sensitivity label which Oracle9i Label Security supports is known as a group. In *The Hunt For Red October* the military organization owning the submarine is an example of a potential group. For example, imagine two groups called *General Operations* and *Special Operations* are defined in Oracle9i Label Security. The *General Operations* group is defined as a child of the *Special Operations* group. In this scenario, personnel authorized for the *General Operations* group will be restricted from viewing information assigned the *Special Operations* group. However, personnel authorized for the *Special Operations* group will be permitted to view information assigned either the *Special Operations* or *General operations* group. The *Special Operations* group provides a larger view of the submarine organization.

- *Group* - The group component is used to record ownership and can be used hierarchically. For example, two groups called *Senior VP* and *Manager* could be created and subsequently assigned as children of the *CEO* group, creating an ownership tree. Users can be given read only or read-write authorizations on an individual group basis, providing powerful row level security.

Reduced Development Cost and Risk Exposure

COTS solution – reduced development cost and risk

One of the key advantages Oracle9i Label Security offers is the fact that the software for row level security is provided out-of-the-box. It allows the developer or administrator to quickly and easily get started with sensitivity labels and row level security. In addition, Oracle9i Label Security enforcement options allow security to be tailored to the specific needs of the enterprise. With Oracle9i Label Security, no development costs are incurred writing the software to enforce row level security. Oracle9i Label Security can thus dramatically shorten the development timeline, resulting in lower development and maintenance costs.

System integrators can bid Oracle9i Label Security as a commercial off the shelf (COTS) solution in proposals.

Optimized Performance

Performance – highly optimized algorithms

Row level security is, by its very nature, an intensive operation. Not only is an access control check performed authorizing access to the database object, but an additional check is performed for each individual data row stored in the database object. The processing required is directly related to the complexity of the security policy. Oracle9i Label Security has been highly optimized to process complex access control decisions based on sensitivity labels. Using the C, PL/SQL and Java software development languages, the Oracle9i Label Security development team optimized the processing based on options selected by the security administrator. The Oracle9i Label Security development team continues to develop and refine sophisticated optimization routines for row level security.

Operating System Independence and Real World Functionality

Designed for standard operating systems, based on stringent government and commercial requirements

The evolution of the Internet and rapid consolidation within the computer industry has made flexibility a key factor in IT expenditures. Oracle9i Label Security is built to meet stringent, real world, operational requirements for row level security found in government and commercial organizations. Oracle9i Label Security is built for today's Internet environment and incorporates years of feedback received from Oracle customers in both government and commercial organizations. Oracle9i Label Security is available on standard, commercially available operating systems, giving IT managers, in government and commercial organizations, hardware flexibility.

Oracle Policy Manager GUI

Manage row level security with a mouse

Oracle Policy Manager is the GUI administration tool for Oracle9i Label Security. Based on the Oracle Enterprise Manager framework, Oracle Policy Manager can be used to define sensitivity labels, establish user label authorizations and protect tables or entire schemes in the Oracle database.

CONCLUSION

The Internet has removed the physical security boundaries which were a byproduct of the old distributed database model. Information which was once stored locally for high speed access is now stored in large central repositories and accessed over high speed modems and fiber optic channels. Oracle9i Label Security introduces powerful new technology to address the new security problems which have developed as the Internet has revolutionized application design and information management. Oracle9i Label Security provides row level security, simplifying applications, reducing application logic and increasing security.

Oracle9i Label Security – Controlling Access to Data
June 2001

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Oracle Corporation provides the software that powers the internet.