Oracle Advanced Security

An Oracle White Paper
[January] [2002]

ORACLE

SECURITY IN BUSINESSES

As more business is conducted on the Web, securing data in motion and user identities is a growing concern. User management and deploying secure infrastructures have bubbled up to the top of database administrator's "Must Do, Must Do it Right" checklist. As Oracle database has grown as the natural choice for activities for data storage, data mining and conducting intelligent business, a variety of secure solutions that address a number of security challenges are also available in the Oracle technology stack.

In the early '90s, client server applications were the rage and had an accelerated growth. There has been a compelling need for data confidentiality and user authentication using secure strong means. By the late 90s, with the explosive growth of the internet and its related commerce, the number of users requiring access to applications exploded as well. Now, user management and administration, ease of use (a k a single sign-on) has naturally become a top requirement for businesses.

Oracle Advanced Security option has met these needs every step of the way with its network encryption, strong authentication and enterprise user management features.

SOLVING SECURITY CHALLENGES WITH ORACLE 9*i* ADVANCED SECURITY

Oracle Advanced Security provides network encryption and several strong authentication mechanisms, single sign-on services, and security protocols while supporting industry standards. The challenges of the database administrator or IT manager that are resolved with the Oracle Advanced Security option can be broken down into three major areas:

- Ensuring the privacy of network data and communications (by integrating encryption and integrity checking)
- Providing strong authentication services for users, databases and web servers (in some cases enabling single sign-on)
- Enterprise User Management (by integrating Oracle Internet Directory and various authentication mechanisms)

DATA/COMMUNICATION PRIVACY

As we know, most of the business communication today is in electronic form, including electronic mail, online sales and purchase orders. Therefore, it is important to protect any such communication from interception and theft. Oracle 9*i* Advanced Security's encryption and data integrity techniques provide data privacy over the wire.

Network Encryption

Encryption is virtually synonymous with computer security. All network traffic is vulnerable to eavesdropping, data capture, replay, data modification and person-in-the-middle attack. The network security features of Oracle Advanced Security address these concerns and protect all data over Oracle*Net.

Advanced Encryption Standard is supported in Oracle *9i* Advanced Security Release 2.

The cryptographic functionality in Oracle Advanced Security converts all clear text into cipher text. Once encrypted, the cipher text is transmitted across the network in a way in which it is computationally unfeasible to convert the cipher text back into its corresponding plain text without the correct key. These encryption services prevent anyone who is able to access your network from reading the data. Oracle Advanced Security provides four proven, well-known algorithms to encrypt Oracle Net traffic:

- Triple DES (3DES, 2Key and 3Key 112- and 168-bit keys)
- RC4 (40-, 56-, 128-, 256-)
- Advanced Encryption Standard (AES)

Each algorithm allows the selection of key lengths. Longer keys produce exponentially stronger encryption. Oracle 9*i* Advanced Security supports 2-key Triple DES with a 112-bit key and 3-key Triple DES with a 168-bit key. It supplies RSA Data Security Inc.'s RC4 with 256-, 128-, 56- and 40-bit keys. While it also provides standard DES with a 56-bit key as well as DES with a 40-bit key, it must be noted that DES is being phased out of use. Starting in Oracle 9*i* Advanced Security Release 2, the latest encryption algorithm, Advanced Encryption Standard, approved by National Institute of Standards and Technology (NIST) is also supported.

Oracle Advanced Security also provides encryption capabilities to thin Java Database Connectivity (JDBC) clients.

Oracle Advanced Security can be deployed in Oracle's Real Application Clusters.

Oracle Advanced Security provides a means of encrypting all Oracle*Net traffic between the database and the client (or a web server) in a standard or Oracle's Real Application Clusters deployment. A key benefit of using Oracle Advanced Security encryption is that the users or the database do not need to have digital certificates or communicate over Secure Socket Layer (SSL).

How about encryption in a web based, 3-tier environment?

Oracle 9*i* Advanced Security's native encryption capabilities can provide end-to-end security at a substantially lower cost

Companies must feel secure about exposing some parts of their internal networks and corporate databases to their partners and customers. HTTP is a stateless protocol that has become the de facto standard in the web based applications deployed by these companies. In this architecture, authentication, privacy and integrity are provided by HTTPS protocol that relies on the principles of public key cryptography. A business considering end-to-end security in this case would need certificates for all the clients, web servers and the database. With the current solutions in the market, the costs could become prohibitive when considering enterprise wide use. End-to-end security using certificates may not be practical and may well be an overkill in certain circumstances.

For example, some businesses, especially those with a Business-to-Consumer model such as an online bookstore may not be interested in client-side authentication as much as providing their customers the assurance that they are indeed placing orders and parting with their credit card numbers to the "real" server and not a spoofed one. This model requires only server side authentication. That is, the client authenticates the server's credentials as part of the initial SSL handshake between the browser and the web server. By configuring Oracle Advanced Security's native encryption between their web servers and the databases allows such deployments to achieve end-to-end security without certificates for all the consumers at a substantially lower cost of ownership.

Data Integrity

While encryption of network traffic ensures data privacy, data integrity protects against data modification and replay attacks. Data integrity proves to the receiver of the message that the message has not been tampered with in transit. This is again a key requirement in today's online world. Data integrity checking—sometimes called cryptographic checksumming—provides *sequencing and hashing* as means to protect against these packet attacks.

Oracle Advanced Security provides industry standard implementations of Message Digest 5 (MD5) or the Secure Hashing Algorithm (SHA-1) for providing data integrity.

STRONG AUTHENTICATION

Oracle Advanced Security provides strong authentication - a means of establishing and verifying the identity of the user - using industry standards including Kerberos, Smart cards, RADIUS, DCE and Digital Certificates.

We have all used passwords as means of authentication to the ATM, to access voice mail or to log into our favorite application. While effective password management policies provide for the possibility of secure passwords, there is a need for augmenting the password based authentication with stronger measures to identify the users. The real question is, how do you prove that the user entering the user name and password is really who she claims to be? Oracle Advanced Security provides several strong authentication schemes while supporting industry standards including Kerberos, RADIUS, two-factor authentication using smart

cards/ token cards/ biometrics, DCE, Entrust Profiles and X.509v3 compliant digital certificates over Secure Socket Layer (SSL).

Oracle Advanced Security strong authentication mechanisms such as Kerberos, DCE and X.509v3 certificates can also provide Single Sign On capabilities to applications that rely on these authentication services.

Kerberos

Oracle 9*i* Advanced Security's kerberos adapter interoperates with MIT KDC, Cybersafe Trust Broker and MSKDC

Kerberos is a network authentication protocol designed to provide secure access in a distributed environment. Working together with a central security service, it uses strong cryptography so that a client and the server can prove their identity to each other over an insecure channel. Subsequently, the client and the server can encrypt all of their communications to assure privacy and data integrity for the rest of their session.

How it works

Oracle Advanced Security's Kerberos integration relies on the trusted central security service (the Kerberos Key Distribution Center) that uses shared secrets to grant "ticket granting tickets" (TGT) for a limited period of time to those clients requesting access to the database. A database connection request from a client submits the TGT to the database which then communicates with the Kerberos Key Distribution Center (KDC) as part of the authentication process, in order to confirm that the TGT is still valid and that it is really a valid user.

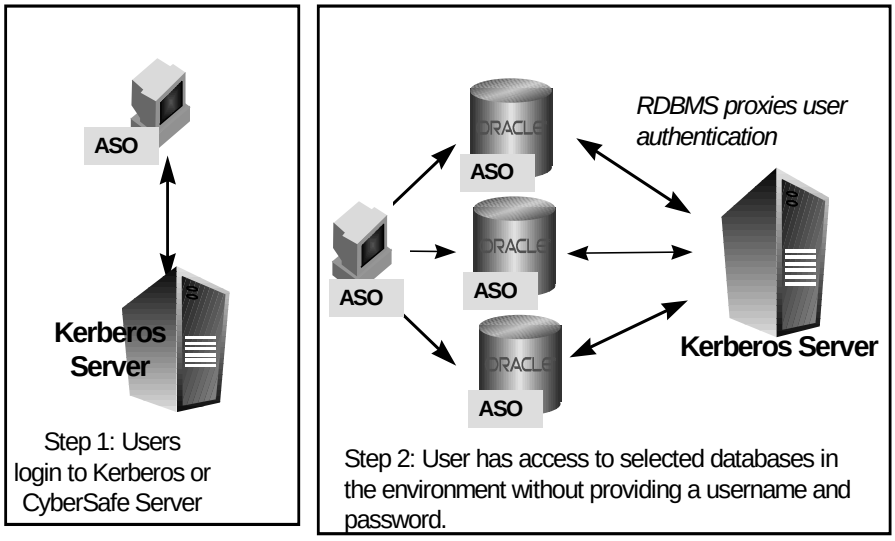

Figure 1

Oracle database client can authenticate using the kerberos tickets granted by MIT Kerberos server, Cybersafe Trust Broker and MIT compliant tickets issued by Windows 2000 KDC. This allows desktop users to possess only a single credential for their Windows and Oracle environment thereby providing a single sign-on solution in a 2 -tier or 3-tier environment.

RADIUS (Remote Dial-in User Service)

RADIUS (RFC #2138) is a distributed system that secures remote access to network services and has long been established as an industry standard for remote and controlled access to networks. RADIUS user credentials and access information are defined in the RADIUS server to enable this external server to perform authentication, authorization and accounting services when requested.

Oracle 9*i* Advanced Security Release 2 supports external RADIUS authorizations

ORACLE RADIUS support is an implementation of the RADIUS Client protocols that enables database to provide authentication, authorization and accounting for RADIUS users. It sends authentication requests to RADIUS server and acts upon the server's responses. The authentication can occur either in synchronous or asynchronous authentication modes and is part of Oracle configuration for RADIUS support.

Oracle Advanced Security 8i and 9i Release 1 provide authentication and basic accounting services to RADIUS users to access the Oracle database. New in Oracle 9*i* Release 2, is the support for external authorizations defined in the RADIUS server.

How it works

When a user requests a database connection, Oracle responds with a challenge to the user. The challenge and the user's subsequent response is sent over to the RADIUS server for verification. The database interprets the RADIUS server's response to allow or deny access to the database. If accounting services are enabled, that process is started right after the connection is granted and terminated upon a connection close request from the user.

Oracle 9i Advanced Security Release 2, allows RADIUS authorizations to be granted to the RADIUS users upon connecting to the database. This is an entirely optional feature that can be configured by the database administrator should businesses have such a need.

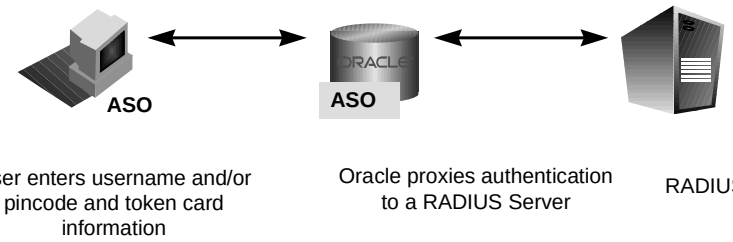

Figure 2

Smart Card / Token Card / Biometric support

Smart cards (such as RSA's SecurID), token cards (such as ActivCard) and biometric authentication that support a RADIUS protocol interface can also be used to authenticate external users to the Oracle database.

These users must be defined as RADIUS users and thereby leverage all the benefits of Oracle's RADIUS support.

DCE

The Distributed Computing Environment (DCE) is a set of integrated network services that works across multiple systems to provide a distributed environment. Oracle DCE Integration has two components

- DCE Communication/Security
- DCE Cell Directory Services Native Naming

Oracle DCE integration provides applications the flexibility to have different levels of integration with the DCE services. That is, depending on the need, applications can choose to integrate very tightly with the DCE services or choose to plug in the other security authentication services provided by Oracle Advanced Security.

Public Key Infrastructure

Public Key Infrastructure (PKI) encompasses technologies, policies and procedures for authentication based on the principles of public key cryptography. The primary components of a PKI are:

Digital Certificates, which are used for identification including users, machines, databases (digital identities)

Public and Private Keys, which form the basis of a PKI for secure communications based on a secret private key and a mathematically related public key

Secure Sockets Layer (SSL), which is the industry standard Internet protocol that is based on public key cryptography principles to provide authentication, encryption and data integrity. SSL supports two authentication modes

- server authentication (to the client)
- mutual authentication (between client and server)

Certificate Authority (CA), which acts as a trusted, independent provider of digital certificates

Additional but nonetheless important components that enable a PKI deployment are secure storage of certificates and keys, management tools to request certificates, administer users, protect their credentials and a directory service that is a centralized repository for user, machine and database identification and authorization.

Secure Sockets Layer (SSL)

Oracle 9*i* Advanced Security has SSL support since Oracle Release 8*i*. New in Oracle 9*i* Release 2 is hardware acceleration support.

The Secure Sockets Layer protocol is widely used over the Internet to give users established digital identities and to prevent eavesdropping, tampering and/or forging messages. SSL support in Oracle Advanced Security encrypts network traffic and provides integrity checking, authenticates Oracle clients and servers, and brings public key-based single sign-on to the Oracle environment. SSL is a stateless protocol that provides encryption and data integrity through the use of cipher suites, which are sets of authentication, encryption and data integrity types. The client and server each have a list of cipher suites they support and upon a SSL transaction initiation, they negotiate the cipher suite to be used for the duration of the connection.

An example of a cipher suite is RSA for authentication with 3DES for encryption and SHA-1 for data integrity. Among encryption algorithms provided by SSL to Oracle Advanced Security option are RC4, DES, and Triple DES. The Triple DES (3DES) algorithm is an extremely strong means of protecting data because it uses more than one 56-bit key employed by standard DES. Triple DES is increasingly being used by organizations such as banks and financial institutions that require strong security. SHA-1 (Secure Hashing Algorithm) provides a means of data integrity checking new to the Oracle environment. It generates a hash to protect data transmissions and ensure that packets have not been modified or tampered with during transmission.

Hardware Acceleration Support

Oracle Advanced Security 9i Release 2, improves the performance of the SSL handshake process by delegating these public key cryptographic operations to a hardware accelerator device using RSA's BSAFE Hardware API.

Secure Storage of Private Keys and Certificates

In order to authenticate, SSL must have a private key and a certificate provided to it. In any Oracle environment, Oracle Wallet is the container that stores this material. The wallet stores the X.509*v*3 certificate, the private key, and additional

data such as trusted certificates, which are processed by SSL. The wallet is additionally protected by a password for tighter security. Any party, users, Oracle databases, and/or Oracle Internet Directory that participate in the SSL transaction must possess a wallet. These credentials are used to authenticate the user to multiple services such as data servers and application servers. The user must remember only one password, which is used to unlock her wallet.

Oracle Wallet Manager

Oracle Wallet can store multiple certificates and is portable across Operating Systems

Oracle Wallet Manager is a GUI tool on the database client that is primarily intended to be used by a database administrator to request certificates from a certificate authority on behalf of users from a certificate authority and provides various wallet management interfaces. The administrator can centrally manage wallet information about applications and databases.

Oracle also provides end users the Oracle Enterprise Login Assistant and the Enterprise Login Assistant Servlet to access their Oracle Wallets and the ability to do simple wallet management tasks.

These tools allow users to achieve single sign-on, simply and transparently, using certificates for authentication.

Entrust Integration

Oracle has made specific product modifications to enable Entrust customers to incorporate Entrust single sign-on into their applications connecting to the Oracle database. These modifications enable Oracle customers to incorporate Entrust-based single sign-on and PKI solutions into their applications. By integrating with Entrust/PKI, Oracle supports customers who deploy applications in a client-server environment and choose Entrust as their PKI vendor.

ENTERPRISE USER SECURITY

Enterprise users are stored and centrally managed in an LDAP-compliant Oracle Internet Directory

E-business has changed how major corporations are conducting business. There is more collaborative work between the company, its customers, suppliers and partners. Companies therefore not only have to administer their employees, but also have the additional responsibility of provisioning partners, customers and suppliers to allow them access to targeted information within the company. Employee turnover, role changes, and the dynamic nature of company relationships are driving up the costs of user administration. In today's business environment there is a need for 24x7 user administration just as there is a need for 24x7 application availability. The costs of user administration soon become prohibitive if the users and their authorizations continue to be duplicated across the different applications that are deployed throughout the enterprise.

Enterprise User Security provides the ability to easily and securely manage enterprise-wide users by

- centralizing the storage of user credentials, roles and privileges in an LDAPv3 compliant directory server
- providing the infrastructure to enable single sign-on using X.509v3 compliant certificates (typically deployed where end-to-end SSL is a requirement)
- allowing password authenticated database users to be centrally managed as password authenticated enterprise users

Prior releases of Oracle Clients that have always supported password based authentication can now be centrally managed in a directory and enjoy the benefits of Enterprise User Security as well. With its reduced processing overhead at the client, improved ease-of-use, and simplified setup and administration, this feature is particularly useful for large user communities accessing multiple applications with passwords.

Enterprise Users can be authenticated using Entrust Profiles starting in Oracle 9i Release 2 of Oracle Advanced Security.

Setting up enterprise user security includes tasks such as creation of global users, enterprise users, enterprise roles and global roles. Most applications are usually designed to have the underlying tables defined in their own schema. There is rarely a need for the application user to have his or her own schema to create their objects. Sharing schema reduces the cost of creating new users to the application as there is no schema specifically dedicated to the enterprise user. Enterprise User Security allows enterprise users to share a common application schema by providing the ability to create a shared schema. Each of these users can have individual roles and they can be audited based on their individual roles.

Enterprise User Security in 9*i*

User Migration Utility assists in migrating database users to Oracle Internet Directory as password-authenticated enterprise users.

Oracle *9i* Advanced Security complements certificate-based authentication with password-based authentication for enterprise users. Password authenticated enterprise users have the ability to connect to multiple databases using a single password. Every enterprise user has a unique identity (called DN) in the directory. The directory stores their database authentication credentials , enterprise roles that hold their appropriate authorizations and shared-schema mapping.

Oracle has traditionally supported password based authentication and therefore, most of the applications that have been deployed allow password authentication. New in Oracle 9*i* release 2 is the *User Migration Utility*, a tool that allows you to migrate databases users into the Oracle Internet Directory (OID) as enterprise users. While easing the administrator's burden with respect to user migration, this utility makes it very easy for the newly created password authenticated enterprise users to continue to log into their applications as usual. Businesses can therefore quickly realize returns by electing to deploy Enterprise User Security.

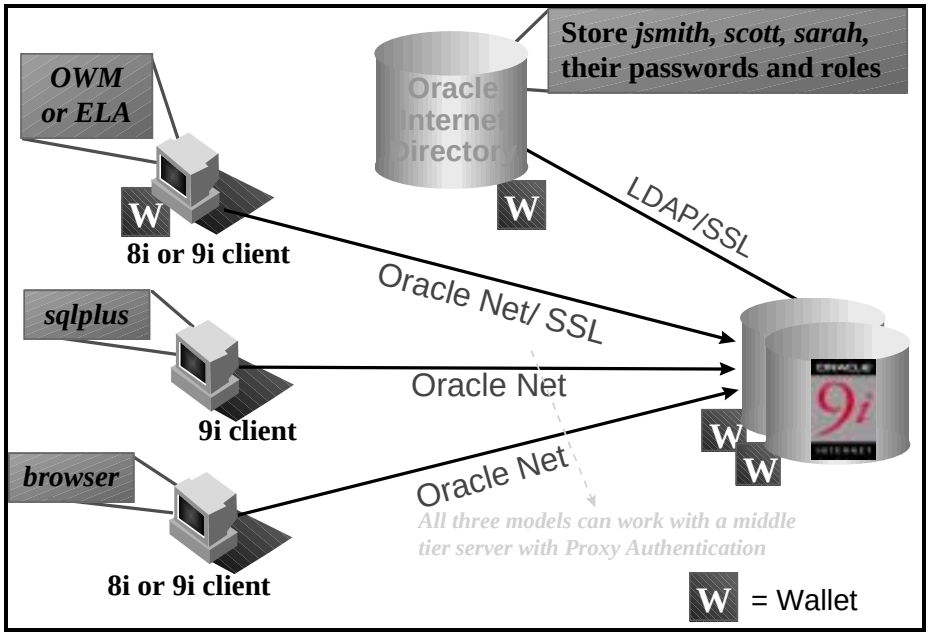

Fig 1 : Enterprise User Security in 9i

The implementation of password-based authentication for enterprise users eliminates the requirement to install SSL and credential management tools on the client.. The communication between the server and the directory is secured over SSL. Thus, the huge overhead of administering certificates to thousands of users is eliminated and the task of configuring SSL and managing wallets is limited to the database server(s) and the Oracle Internet Directory.

Certificate Based Authentication of enterprise users requires client side SSL in addition to the SSL requirement on the directory and the server. Using certificates provides single sign-on capabilities across applications that are PKI -enabled.

For password and certificate based authentication, the security administrator primarily uses the following tools to administer users :

- Enterprise Security Manager - to create users, roles and set the database password.
- Oracle Wallet Manager - to create wallets for the users, directory and the server(s) and enable autologin.
- Oracle Directory Manager - to facilitate directory deployment.

A password authenticated enterprise user still has the responsibility of following good password management guidelines. The two tools available for this task are the Oracle Enterprise Login Assistant and the ElaServlet. The Enterprise Login

Assistant also provides single sign-on for the certificate authenticated enterprise user when the user uses this tool to login.

Three-Tier Enterprise User Security

Enterprise User Security extends to three-tier environments in Oracle 9*i* release.

N-Tier authentication, sometimes referred to as proxy authentication, allows the application users to retain their identity even as the application uses a generic login credential to authenticate various users. For example, Mary and Jane, both HR managers, may be responsible for two different divisions in the same company. A typical HR application authenticates the individual user, derives the user's privileges and for improving performance, makes connections to the database as a generic HR_APPUSER. By extending n-tier authentication to enterprise users, Mary and Jane now experience not only granular access control, but also improved performance. The generic HR_APPUSER can be set up (using programmatic interfaces) to provide efficient connection pooling and only switch the context on behalf of Mary and Jane. Since the context is retained the enterprise users, Mary or Jane whose connections are proxied, can also be audited.

Enterprise Users and other Oracle products

Enterprise Users can be configured to be SSO users. VPD policies can be applied to these users and they can be audited as well.

Single-Sign on has evolved as the poster child of usability in a web based computing model. Starting in Oracle 9iASv2, Oracle Forms and Oracle Reports can participate in single-sign on using Oracle 9iAS Single Sign On Server. In order to accomplish this task, the users are centrally administered in Oracle Internet Directory. It is possible to configure these users as Enterprise users in order to leverage shared schema, enterprise roles and other benefits of being an "Enterprise User".

Security features offered by the Oracle database including Fine Grained Access Control and Auditing can be used in conjunction with Enterprise Users.

Enterprise User Security in 8*i*

Oracle Advanced Security Release 8*i* relies on SSL everywhere (client, server and the directory) , centralized user and authorization management to provide single sign-on solution. Oracle Wallets that store the X.509v3 certificates are required for the enterprise users, database server(s) that can be accessed and the Oracle Internet Directory.

It provides end-to-end security over SSL. Oracle Wallet Manager provides the ability to request and manage certificates. Once the Certificate Authority issues the certificate, Oracle Wallet Manager allows you to import it into the Oracle Wallet.

For businesses that do not already have PKI requirements or deployed PKI, the task of requesting and managing X.509v3 certificates for all their users is overwhelming and turns out to be a huge overhead. Password authenticated enterprise users in Oracle Advanced Security 9i release, eases this burden.

Enterprise User Security concepts

Database Users vs. Enterprise Users

Users are typically defined in the database using the following syntax -

CREATE USER *jsmith* IDENTIFIED BY *changeonlogin*;

This creates a database user who authenticated to the database using his/her password who can then access the database using the following syntax:

sqlplus jsmith/changeonlogin@db_service_name

User 'jsmith' has to be created in every database that he needs to access and he can potentially have different passwords in each of these databases. His privileges in a database are controlled by the local roles that are granted to him in that database.

An enterprise user, on the other hand, is provisioned in the LDAPv3 compliant Oracle Internet Directory server (OID) using Enterprise Security Manager GUI tool. Enterprise users have a unique identity in the directory , the Distinguished Name(DN). When an enterprise user attempts to connect to the database, the database should be able to identify him/her as an enterprise user. To facilitate this process, enterprise users are defined as global users in the database. A global user is created using syntax such as -

create user jsmith identified globally by "cn=jsmith, c=us, o=acme, dc=com";

When this user requests database connection using

sqlplus jsmith / @db_service_name

the database recognizes this user to be a global user and defers the authentication to the directory.

Enterprise Roles

Enterprise Users are given privileges via Enterprise Roles

Since the database does not locally store the detailed information about an enterprise user, it also has no knowledge about his or her enterprise roles and privileges. Enterprise roles are defined in the directory and act as the intermediary to indirectly grant global roles to the enterprise user. They are containers for one or more global roles defined in the database. An enterprise role can contain global roles that are defined in different databases. This feature is extremely powerful as it provides the ability to centrally manage enterprise roles that are assigned to thousands of users on one hand and map to multiple global roles across many different databases. It eliminates the administrative hassles involved in creating, adding and revoking new roles from/to each and every user in each and every database that is accessed.

Enterprise Roles are created using Enterprise Security Manager.

Global Roles allow you to group various object privileges to allow easy assignment to enterprise roles

Global Roles

Global roles are defined in the database and known only to the database they are defined in. However, authorizations to use these global roles are stored in the directory (using enterprise roles) when you are deploying Enterprise User Security. Global roles are defined in the database using

CREATE ROLE *hr_manager* IDENTIFIED GLOBALLY;

Global roles cannot be granted in the database to any user. They are assigned or de-assigned to an enterprise role only in the directory using Enterprise Security Manager. This is a very subtle difference between global roles and the other system or object privileges that are granted in the database to the user .

Enterprise Domains

Businesses today have a large number of databases. These database entries can also be stored centrally in a directory server . Each database is identified by its unique distinguished name (DN). Enterprise domain is the imaginary boundary to group these databases in a meaningful manner. For example, there should be different access control lists that restrict access to the HR database and ORDER database. One of them could be configured to allow password authenticated users while the other could be configured to allow only certificate based authentication. Therefore, the HR and ORDERS databases are better protected when placed in different domains. Current user database links that enable a user on one database to execute procedures in the remote database as the object owner, require the databases in question to be in the same enterprise domain. Enterprise Domain defines the scope of an enterprise role and the mapping object (mapping enterprise users to the shared schema).

Implementing shared schema is the key to lower your user administration costs

Shared Schema

Business applications have a number of users who should be allowed access to information only through the business application. For example, business application users Mary and Tom need the ability to create orders and employees in the database but they should not have the ability to create ORDERS/SHIPMENTS or EMPLOYEE/DEPARTMENT tables. In fact, they should not be allowed to create new objects in the database. Shared schema provides the means to address this issue.

A shared schema is created using

CREATE USER APPS_SCHEMA IDENTIFIED GLOBALLY AS ‘’;

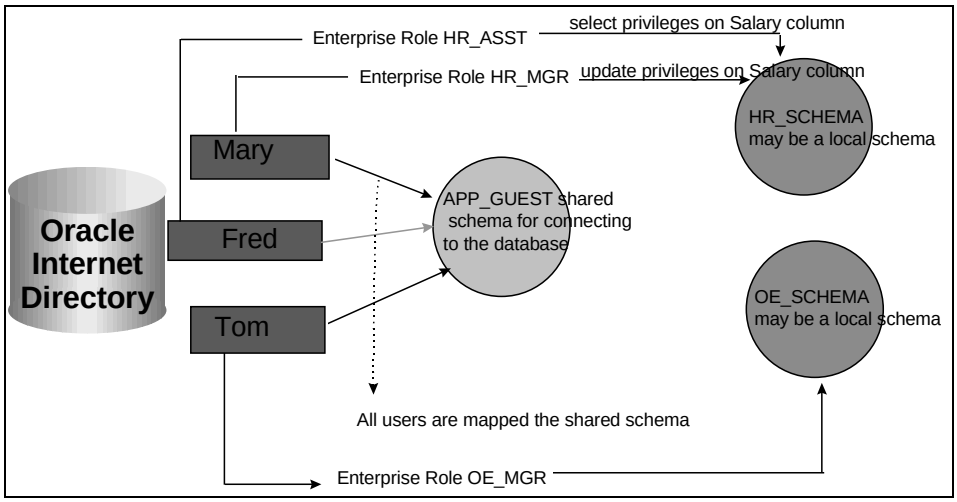

Fig2 : Enterprise Users using Shared Schema

Enterprise users are mapped to the shared schema in the directory. All users that are mapped to a shared schema own all the objects in that schema. For example, Mary and Fred mapped to APP_GUEST schema have access to all objects in that schema. So, it is prudent to not create objects directly in this APP_GUEST shared schema. Instead each application should have its schema. HR application and Order Entry application should be designed to use HR_SCHEMA and OE_SCHEMA respectively. For example, Mary can be assigned HR_MGR enterprise role that is the container for HRMANAGER global role with update privileges to the salary column.. Fred on the other hand, can be assigned HR_ASST enterprise role, a container for HR_ASSISTANT global role. Similarly another user, Tom, who needs Order approval privileges can be created as an enterprise user , mapped to the APP_GUEST shared schema and assigned ORDER_MGR enterprise role (which is a container for ORDER_MANAGER global role). Thus, we can preserve granular access control and have simplified user administration at the same time.

APP_GUEST shared schema is the shared resource that all the mapped users connect to upon being authenticated to the database. Keeping this shared schema devoid of objects and local roles, protects the HR and OE application data from being accessed or manipulated outside the business application.

Current User Database Link

It is conceivable that certain procedures in an application need to be executed only by a user with a certain authority. For example, assume that a stock option grant needs to be executed as a certain privileged user, HR_STOCK_APPROVER. Using Fixed User Database Links is one solution. However, it means storing the user's credentials with the link definition in the application database. A more secure solution is to define the privileged user as a global user. When the

application user accesses this function, the procedure executes as the object owner who is defined in the directory.

Keeping User Management simple

Centralized user credentials and authorization management reduces the user administration costs as there is only one single source of truth that needs to be maintained Extending Enterprise User Security to password authenticated users allows businesses to secure access to their applications while lowering administration costs for their current implementations of business applications as well. Enterprise User Security also provides end-to-end security over SSL using X.509v3 certificate based authentication to the database. Enterprise users can be authenticated using Entrust P12 files in Oracle 9i Release 2 of Oracle Advanced Security.

CONCLUSION

Network Encryption, Strong authentication and Enterprise User Security are all available with Oracle 9*i* Advanced Security.

Oracle 9*i* Advanced Security solves the security challenges of businesses by providing industry standard network encryption and data integrity algorithms, and strong authentication using industry standards including Kerberos and Digital Certificates. Finally, businesses enjoy centralized and secure user administration with Enterprise User Security.

Oracle Advanced Security
[January] 2002
Author: Sudha Iyer
Contributing Authors:

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