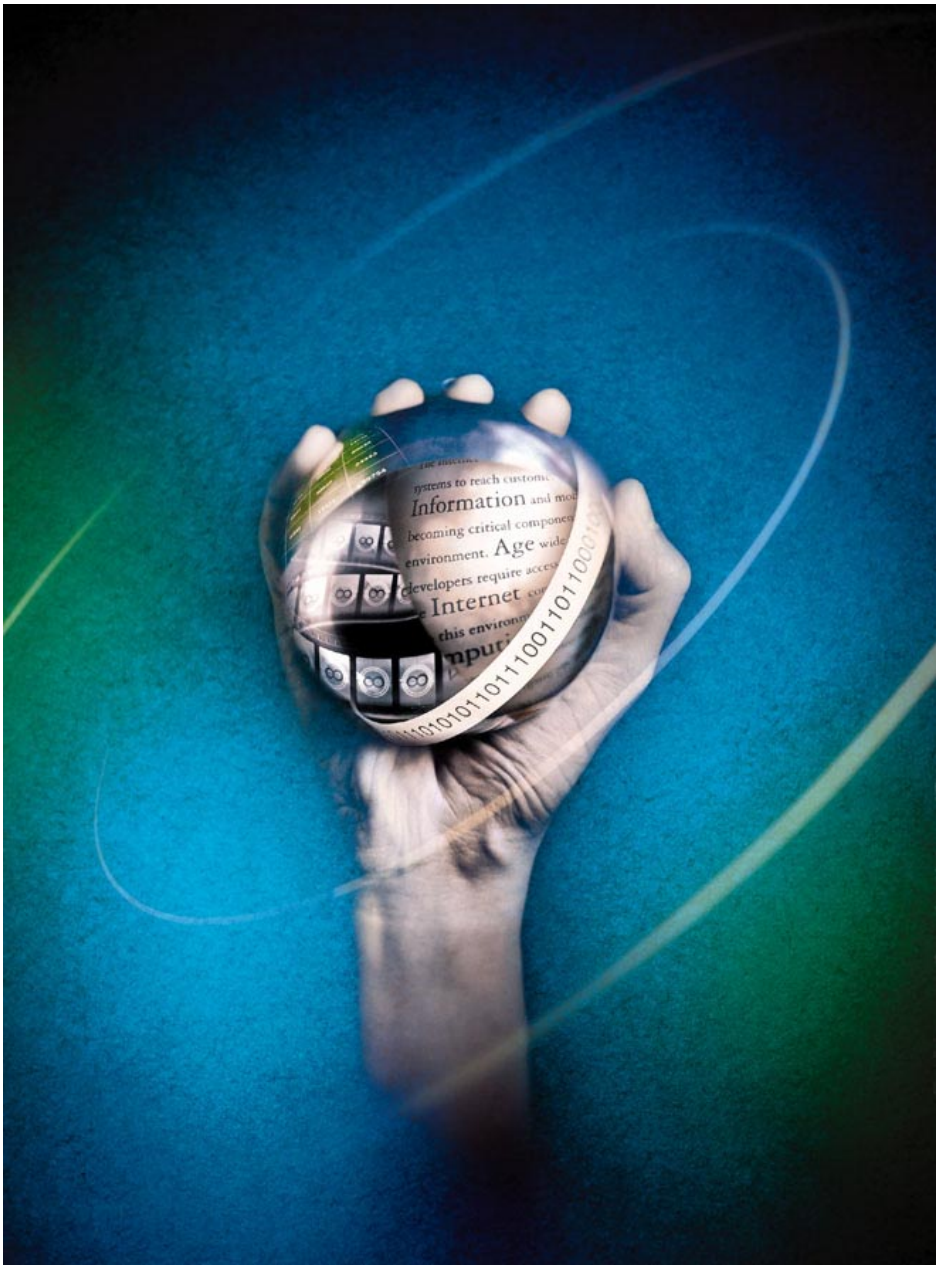
Oracle8*i*™ and Internet Security

An Oracle Business White Paper

November 1999



SECURITY CHALLENGES OF THE INTERNET

THE DISINTERMEDIATION OF SECURITY

One of the primary benefits of extending the business Enterprise to the Internet is disintermediation, a reduction in the supply chain between a customer and a business. As a result, organizations are better able to serve their customers, and to gauge their needs and preferences. Customers get faster access to information, goods and services. Organizations save money by "cutting out the middleman," and can potentially increase revenues by using the Internet as a sales channel. These factors all combine to make doing business on the Internet extremely compelling for organizations.

Whether the Internet represents a web-front store, or a way of computing, the disintermediation of security, is a potentially serious risk of doing business on the Internet. Consider an order entry application moving from a client-server deployment in-house, to a web-based storefront. In the former case, people accessing the application are known to the company and are trusted to handle orders for multiple customers, orders which they take over the phone. There are many "layers" of security involved, from the telephone itself (which is reasonably secure against tampering or eavesdropping), to the employee herself, who is using an application accessible only within the organization, that allows her to review multiple customers' orders. Both the employee and the application are thus largely trusted by the company. While strong access control mechanisms are required, these access control mechanisms are generally embedded within the application itself and are not very granular, since a single order entry clerk typically enters orders for multiple customers.

Now those applications, once staffed by in-house personnel, have become self-service web-based applications, so you can no longer put all your trust in a privileged user accessing a privileged application. Instead of an employee entering, manipulating, and altering data for multiple customers, customers may place their own orders and access them directly. As a result, access control must be far stronger and more granular than in a strictly intranet application. For

example, if customers access their orders directly over the Internet, an organization needs to ensure that customers only see their own orders, and not those of any other customers. The result of the disintermediation of security is that thousands of potentially unknown users may access mission-critical data directly, instead of a limited group of known users accessing data only
within the Enterprise.

OPEN NETWORKS ARE INHERENTLY INSECURE

Another security challenge of doing business on the Internet is that open networks are inherently insecure, because data can be read in-transit by virtually anyone, friend or foe. Suddenly, your most valuable data, including business transactions, customer data and information, is passing over insecure networks. Organizations that feel perfectly comfortable allowing business plans to travel from client to server, or application server to data server inside their internal networks, feel far differently about allowing those plans to travel through the Internet. Companies who seek to harness the Internet to conduct business must take steps to ensure both the confidentiality of their data and the integrity of their data.

CONSTRAINTS OF THE INTERNET

The range of possible solutions to these security challenges is further constrained by the nature of the Internet itself. Doing business over the Internet, particularly business-to-business transactions, involves communication between disparate networks, therefore, solutions must be open and interoperable. Otherwise, organizations can, at best, deploy one-off, proprietary virtual private networks (VPNs), which cannot truly harness the Internet. Furthermore, any security solutions must be scalable, to handle hundreds of thousands of connections and hundreds of thousands of users. Of course, these solutions must also be manageable.

KNOW YOUR USERS

A solution to the Internet security challenge posed by thousands of potentially unknown users is a simple one: "know your users." "Know your users," however, encompasses multiple elements, including strong authentication (knowing who a user is) as well as authorizations (limiting what a user can do). Additionally, these security mechanisms must be applied within the three-tier environment typical of Internet applications: client or thin client to application server to data server.

STRONG, STANDARDS-BASED AUTHENTICATION

A popular and important Internet security standard is the Secure Sockets Layer (SSL) protocol. SSL uses digital certificates and a public key infrastructure (PKI) to provide the major pieces of security: authentication of people and machines, encryption techniques for privatizing, and checksums for protecting against data modification or snooping. The importance of verifying the identity of not only users, but also of machines, becomes crucial when an organization opens its doors to the Internet. Most organizations have chosen to protect their databases by keeping them inside of the network and placing a web server outside of the network. Used in combination with a firewall and other security measures, the data can remain safe. The data server's ability to authenticate the web server, therefore, is extremely important. You must verify that the web server is what it claims to be, so that you can trust it to pass data — encrypted or unencrypted — to the outside world. SSL provides the critical authentication piece along with the data privacy piece of the security solution.

SSL uses industry-standard X.509 certificates for authentication. Oracle's implementation of SSL, both in Oracle® Application Server and in Oracle8*i*, takes advantage of X.509 version 3 certificates. An X.509 certificate is analogous to a driver's license containing a user's identifying information.

In Oracle8*i*, SSL works in the following manner: a client is issued an X.509 certificate and a private key which is stored in an Oracle Wallet. When the client initiates a Net8™ connection to the server, SSL performs a handshake between the two processes using the private key and

certificate. If it is successful, the client is granted access. This handshake is transparent to the user.

Oracle Application Server supports SSL authentication for both HTTP, and IIOP (the Internet Intra-ORB Protocol); in the former case for web client and web listener authentication, and in the latter case for CORBA client and ORB authentication. In both cases, the standard SSL options of anonymous (no authentication), server-only authentication, and mutual client-server authentication are supported. Server-only authentication requires that the server have an X.509 certificate installed and that the client have the appropriate root data (the public key from the certificate authority (CA) which generated the server certificate) so that the client can verify the server certificate. Mutual authentication requires both client and server have certificates and appropriate roots installed.

Oracle environments doing business over the Internet can have assurance in the strong, standards-based authentication of users, because both Oracle8*i* and Oracle Application Server both support SSL-based authentication of users as well as servers.

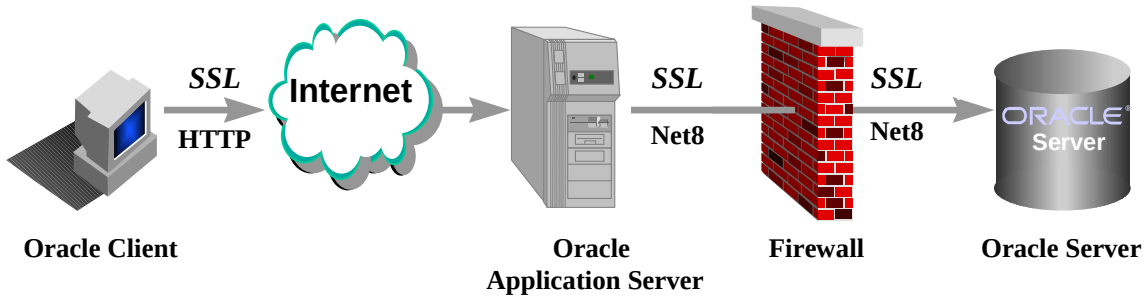


Figure 1. SSL Secures Oracle and Internet Communications

PRESERVING USER IDENTITY

In order to "know your users" in an Internet environment, an organization must be able to preserve the identity of the real user through the tiers of an application: from client to application server to data server. If the application server (or other middle tier) connects to the database as a super-privileged user, the application server can perform all actions on behalf of all users, which loses the desired individual identity and accountability. However, in order to

exploit the connection pooling offered by many application servers, the challenge becomes preservation of the user identity through the middle tier, without the overhead of setting up a separate authenticated user connection from the application server to the data server. After all, the middle tier will have authenticated the user, and can authenticate itself to the data server; therefore, it's simply not necessary re-authenticate the user all the way through to the data server!

For these environments, Oracle8*i* provides "lightweight session" creation via the Oracle® Call Interface; applications can have multiple user sessions within a single database session. These "lightweight sessions" allow a middle tier to create a session on behalf of the "real" user, without the overhead of a separate database connection, thus preserving the identity of the real user through the middle tier. While the middle tier authenticates itself to Oracle8*i*, the "real user" need not be re-authenticated, and can "piggyback" on the initial application server connection. Another benefit is that middle tier applications no longer need to store and retrieve database passwords for users.

Oracle8*i* also avoids the problem of the "super-privileged" application server, by limiting the ability of middle tiers to initiate connections on behalf of users. For example, the "WebStore" application server could be privileged to create a lightweight user session for Fred using Fred's "customer" role only, but not create sessions for Marie.

Oracle8*i* enhances accountability by enabling organizations to audit actions taken *on behalf of* the "real" user by the middle tier. Oracle8*i*'s audit records capture both the logged-in user (i.e., the "WebStore" application server that initiated the connection), and the user on whose behalf an action is taken. Auditing user activity, whether users are connected through a middle tier or directly to the data server, enhances user accountability, and thus the overall security of three-tier systems.

RADIUS SUPPORT

RADIUS is another key element in knowing the identity of users accessing the Enterprise remotely. The RADIUS (Remote Authentication Dial-In User Service) protocol is an industry standard for remote authentication and controlled access to networks; it is implemented by

almost all organizations that allow remote user access. Many Enterprises have standardized on RADIUS because of its widespread acceptance in the industry, its flexibility, and its ability to provide user authentication, authorization, and accounting between a network client and an authentication server, as well as centralizing all user information in order to ease and reduce the cost of user administration.

RADIUS support to Oracle8*i* is provided through the Advanced Security Option, and offers two major benefits for Oracle users. First, it readily integrates into existing systems, by making the Oracle8*i* data server a RADIUS client, therefore capitalizing on the infrastructure and investment that organizations have already made. Second, it extends the solutions for authenticating users to Oracle by enabling support for new authentication technologies such as token cards, smartcards and challenge-response mechanisms. With very little development effort required by a technology provider, Oracle customers' choices of authentication mechanisms are extensively expanded.

The Advanced Security Option already interoperates with a number of authentication services provided by third-party vendors with technologies such as token cards, Kerberos implementations, and biometric devices. With RADIUS, support for any *new* authentication services is built-in to Oracle. RADIUS allows the network equipment vendor (Oracle) to support one authentication protocol (RADIUS) on the server, while authentication vendors supply the specific RADIUS server. Little development effort is required by the technology provider, and more authentication solutions — such as smartcards — are available with enhanced features such as accounting and challenge-response methods of authentication, and accounting, two services that have never before been supported.

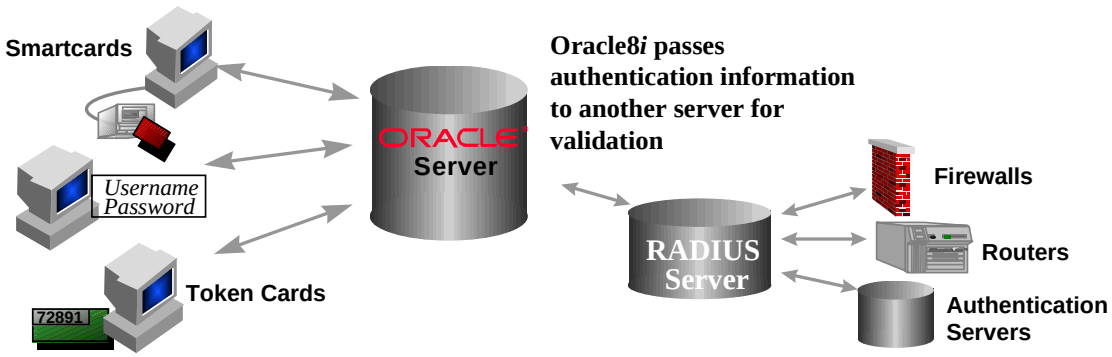


Figure 2. RADIUS Integration In a Network With Oracle, Remote Access, and Strong Authentication

CONTROL USER ACCESS

Extending the Enterprise to the Internet may potentially expose an organization's valuable, mission-critical data to *any* user accessing the network from the Internet, because the disintermediation effect of the Internet also reduces the layers of security between a user and the data the user accesses. Therefore, organizations seeking to extend the Enterprise must implement strong, data-driven, user-based access control, that extends from the client through the application server, to the data itself.

THE VIRTUAL PRIVATE DATABASE

Giving customers and partners direct access to mission-critical systems over the Internet may yield reduced cost, better service, and more timely information, but it also offers new challenges. Organizations must not only keep data safe from prying eyes, but they must segregate data appropriately, often to the level of individual customers or users. Also, many companies are interested in providing Internet "hosting" environments, with a well-designed and well-managed computing infrastructure, but must keep the data of each "hosted" corporation separate and secure from each other, while allowing customizations and data access methods which best meet their individual needs.

Oracle8*i* sets a new standard in security with the introduction of the Virtual Private Database: server-enforced, fine-grained access control, together with a secure application context, enabling multiple customers and partners to have secure direct access to mission-critical data. The Virtual Private Database enables, within a single database, per-user or per-customer data access with the assurance of physical data separation. For Internet access, the Virtual Private Database can ensure that online banking customers see only their own accounts, and that web storefront customers see only their own orders. Web hosting companies can maintain multiple companies' data in the same Oracle8*i* database, while allowing each company to see only its own data.

Within the Enterprise, the Virtual Private Database results in a lower cost of ownership in deploying applications. Security can be built once, in the data server, rather than in each application which accesses data. Security is stronger, because it is enforced by the data server,

no matter how a user accesses data. Security is no longer bypassed by a user accessing an ad hoc query tool or new report writer.

The Virtual Private Database is enabled by associating one or more security policies with tables or views. Direct or indirect access to a table with an attached security policy causes the data server to consult a function implementing the policy. The policy function returns an access condition known as a predicate (a WHERE clause) which the data server appends to the SQL statements, thus dynamically modifying the user's data access. A secure application context enables access conditions to be based on virtually any attributes an application deems significant, such as organization, cost center, account number, or position. For example, a human resources application may base its security on "organization," "employee number," and "position;" that is, a user in the "manager" position can see the employee records of all employees in his "organization," while a user in the "employee" position can only see and update records matching his own "employee number."

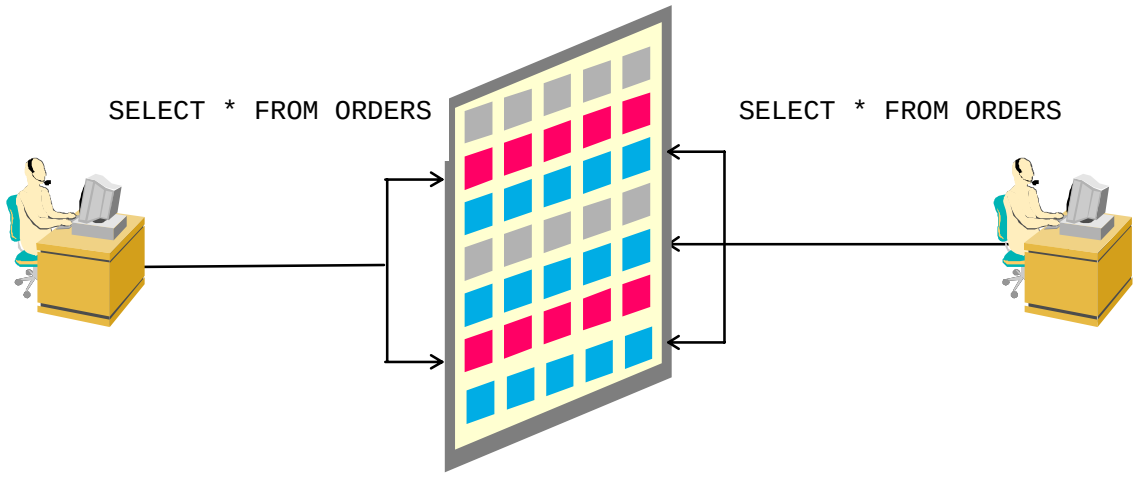


Figure 3. The Virtual Private Database: Customers View Their Own Orders Only

The Virtual Private Database ensures that, no matter how a user gets to the data (through an application, a report writing tool or SQL*Plus®) the same strong access control policy is enforced. The Virtual Private Database can help banks ensure that customers see their own

accounts (and nobody else's), that telecommunications firms can keep customer records safely segregated, and that human resources applications can support their complex rules of data access to employee records. The Virtual Private Database is key enabling technology in opening mission-critical systems to partners and customers over the Internet.

SECURE APPLICATION ROLES

As organizations open their mission-critical systems to the Internet, it is imperative that they control not only what a user may access, but how a user may access it. For example, an organization deploying a web storefront application must ensure that any privileges the user employs in the back-end order entry database are only enabled within the web storefront application. To address this need, Oracle8*i* introduces the secure application role, a role which can be enabled *only* through an application.

Oracle8*i*'s secure application roles enable security in thin client or web-based applications by ensuring that the privileges enabled within the middle tier are only enabled within the application. Application roles are defined in Oracle8*i* such that an application can validate a SET ROLE command (using any desired criteria) prior to allowing SET ROLE to succeed. Oracle8*i* ensures that it is a trusted package — a secure program element — enabling the SET ROLE command. For example, Oracle8*i* can ensure that the user is connected through an application server proxying the user's identity to the database, and that the user is not connected to the database directly (and thus invoking the role outside of the application). All database privileges the user needs may be granted to the application role; as a result, the user can't access any data *except* within the application.

Prior to secure application roles, system security officers who wanted to ensure that users only enabled roles through applications (and not directly in the data server) had to rely on "security by obscurity" to obtain this functionality. You could embed a role enabled by password within an application (for which the users who are granted the role did not know the password), but the password needed to be supplied by the application in some way, e.g., by burying the password within the application.

Secure application roles are key enabling technology in extending the Enterprise to the Internet, because they can ensure that users only access data through your Internet applications.

INTEGRATED SECURITY AND DIRECTORY SERVICES

An inherent challenge of any distributed system is that common application information — including user information, such as mailstop, organizational unit and a user's digital certificate — is often fragmented across the Enterprise, leading to data that is redundant, inconsistent, and expensive to manage. Directories are being viewed by an increasing number of Oracle and third-party products as the best mechanism to make Enterprise information available to multiple different systems within an Enterprise. Directories also make it possible for organizations to access or share certain types of information over the Internet, for example, through a virtual private network. The trend towards directories has been accelerated by the recent growth of the Lightweight Directory Access Protocol (LDAP).

A specific type of Enterprise information which is commonly proposed for storage in a directory is privilege and access control information. Both user privileges, represented as roles, and object constraints, represented as Access Control Lists (ACLs) listing those users who may access an object, may be stored in a directory. Oracle Application Server is currently capable of storing and accessing, in one or more LDAP directories, ACLs for objects on the application server.

Similarly, Oracle8*i* supports Enterprise roles: centrally-administered privilege sets, maintained in Oracle Internet Directory, or any other LDAP-compliant directory. Enterprise roles enable strong, centralized authorization of users. Also, an administrator can add capabilities to Enterprise roles (granted to multiple users) without having to update the authorizations of each user independently. Oracle Security Manager (an extension to Oracle Enterprise Manager) provides one tool to centrally manage user definitions and assign Enterprise roles, resulting in a lower cost of user administration throughout the Enterprise. Another benefit of single station administration is that if security is easy to administer, organizations are more likely to implement strong security throughout the Enterprise.

Oracle Internet Directory, integrated with multiple Oracle products, is a native LDAP version 3 implementation that combines the mission-critical strength of Oracle's database technology with the flexibility of the Internet standard. Oracle Internet Directory is the default data repository for accessing Oracle8*i* Enterprise user information, including X.509 certificates, and Enterprise roles.

Centralized user and privilege management provides multiple benefits to organizations deploying Internet-based applications. Common information can be readily accessed by individuals who need it. User privileges may be centralized and thus secured. Eventually, Oracle users will be completely directory-based, meaning that organizations can support hundreds of thousands of users, merely by defining a user once in a directory server, providing the scalability and manageability required for Internet applications.

PROTECT DATA IN THE NETWORK

The security challenge posed by the insecurity of data transmission over the Internet can be met by the data confidentiality and integrity mechanisms offered by secure networking protocols. The Secure Sockets Layer (SSL) protocol was developed by Netscape Corporation to prevent eavesdropping, tampering with, or forging messages over the Internet, and is widely-used over the Internet to give users established digital identities. SSL is the leading security protocol for the Internet, and it provides data encryption, data integrity, and client and server authentication to secure all sessions.

SSL SUPPORT IN ORACLE

Oracle Application Server supports Secure Sockets Layer (SSL) to protect data privacy between the browser and the application server, as well as authenticating the application server and, optionally, the user. Oracle Advanced Security for Oracle8*i* (formerly known as the Advanced Networking Option) also supports SSL, to ensure data privacy and integrity between web servers and corporate data servers. These two products together provide an end-to-end solution for the privacy and integrity of data flowing through networks and across the Internet.

SSL secures not only Net8 connections to the data server, but other protocols such as IIOP, LDAP and HTTP. By capitalizing on Java™ support, Oracle Advanced Security secures IIOP connections, giving Oracle the ability to work with thin clients and Enterprise JavaBeans™ (EJB). SSL both encrypts network traffic and authenticates Oracle clients and servers. By using SSL, Oracle servers can authenticate users by utilizing standard X.509 version 3 certificates. The inclusion of SSL in Oracle Advanced Security expands support for encryption and provides public key authentication based on the SSL standard.

SSL provides encryption and data integrity (also called checksumming) through cipher suites. Cipher suites are sets of authentication, encryption and data integrity types. The client and server each have a list of cipher suites they support and they negotiate which one is to be used during connection. Oracle Advanced Security offers choices of encryption, such as DES and RC4. Among the encryption provided by cipher suites is Triple DES. Because it uses more than one 56-bit key employed by standard DES, Triple DES is a considerably stronger means of protecting data. Triple DES is increasingly being used by organizations requiring strong security.

Support for SSL in Oracle Advanced Security closes the loop for secure end-to-end communications between any client, a web server or application server, and an Oracle8*i* data server. The addition of Oracle Application Server in the Oracle environment provides end-to-end

network security.

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

Worldwide Inquiries:
+1.650.506.7000
Fax +1.650.506.7200
http://www.oracle.com/