Oracle White Paper
October 2010

Oracle Advanced Security with Oracle Database 11g Release 2

ORACLE

Introduction

Protecting personally identifiable information (PII), intellectual property, financial results, and other sensitive information is a top priority for all organizations. Universities, healthcare organizations, and retailers are just a few of the organizations that have vast amounts of sensitive data ranging from social security numbers to personal health information (PHI) to credit card numbers. The amount of sensitive information collected and transmitted will continue to increase dramatically as organizations strive to achieve increased efficencies and consumers continue to embrace Internet based commerce. At the same time, the value of sensitive information to those attempting to commit identity theft and other types of fraud continues to increase. Over the past years, the number of reported data breaches has increased, resulting in damages reaching into the tens of millions of dollars. As a result, numerous privacy and breach notification laws have been put in place that mandate the use of encryption technologies to provide a defensive shield for sensitive data: In 2003, the U.S. State of California passed the first such law known as Senate Bill 1386 (extended by Assembly Bill 1950). Ever since, similar laws have been put in place across the U.S., the State of Massachusetts being the most recent. The payment card industry data security standard (PCI-DSS) is an industry driven initiative that mandates the use of encryption technology to provide protection for credit card data stored by anyone who processes credit card transactions. The HiTECH act of 2010 adds breach notification procedures to the Health Insurance Portability and Accountability Act (HIPAA), which only required encryption when sensitive information is transmitted across public networks (e.g. the Internet). Oracle Advanced Security provides transparent, standards-based security that protects data through data-at-rest encryption, network encryption, and strong authentication services.

"Valuable content belongs in a secure, central database where it can be easily managed, automatically backed up—ideally, with minimal man hours. There is nothing more important to us than our customer's content, which is why we chose Oracle to secure our information and support our growth strategy."

Andy Barrett, Chief Technology Officer, Yuntaa

Oracle Advanced Security

Oracle Advanced Security transparent data encryption (TDE) provides the industry's most advanced database encryption solution. TDE automatically encrypts data written to storage by the Oracle database and automatically decrypts the data after the requesting user or application has authenticated to the Oracle database and passed all access control checks including those enforced by Database Vault, Label Security and virtual private database. Database backups retain the data as encrypted, providing protection for backup media. Data exported into flat files from the Oracle Database can be encrypted as well. Both logical and physical standby databases can be configured with TDE to provide complete protection for sensitive data in high availability architectures. Advanced Security network encryption provides both SSL based and native network encryption capabilities to protect data in transit. Advanced Security strong authentication services support PKI, Kerberos and RADIUS for an alternative to existing password-based authentication.

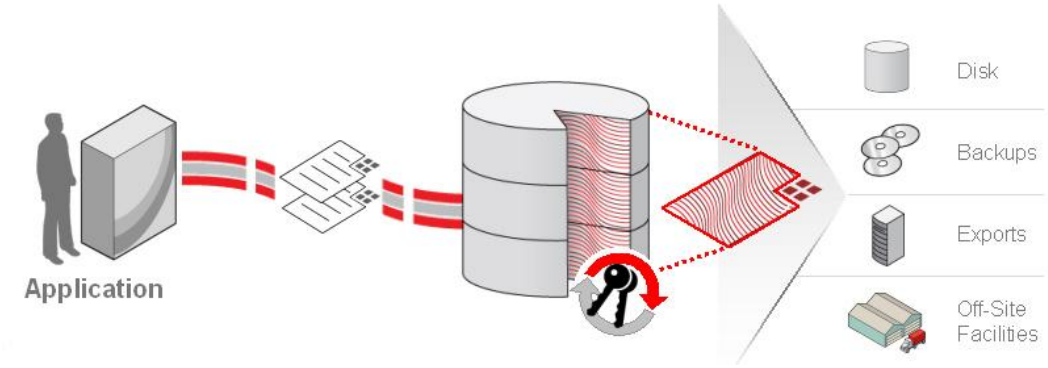

Figure 1: Oracle Advanced Security Transparent Data Encryption

Transparent Data Encryption

Oracle Advanced Security TDE provides both encryption of application *tablespaces* as well as individual application table *columns* such as credit card and social security numbers. TDE tablespace encryption eliminates the complexities of identifying and encrypting individual columns and achieves increased efficiencies resulting in higher performance. Customers upgrading to Oracle Database 11g can choose to skip the process of identifying which columns to encrypt and simply use TDE tablespace encryption to protect entire application tablespaces. All data stored in encrypted tablespaces will be automatically encrypted. Data that is stored in temporary and 'undo' tablespaces as well as redo logs is encrypted as well. When the database is backed up, the encrypted files remain encrypted on the destination media, protecting the information even when the backup media is lost or stolen. TDE tablespace encryption works seamlessly with Oracle Streams, Oracle Data Guard, Oracle Advanced Compression, Oracle Exadata Smart Scans and Exadata Hybrid Columnar Compression (EHCC). Storage savings achieved as a result of compression remain the same because data is encrypted after the compression process completes.

Support for hardware-based encryption acceleration

Transparent Data Encryption has a very low performance impact of less than 10% for most transactional applications. Oracle Database 11g Release 2 (11.2.0.**2**) TDE tablespace encryption provides stored data protection with near-zero performance impact by automatically detecting and utilizing the hardware-based cryptographic acceleration available in the new Intel® Xeon® 5600 CPUs (AES-NI); with this, encryption and decryption is 8 to 10 times faster. Patch 10080579 is required to accelerate the encryption process; decryption acceleration is available by default. TDE column encryption currently does not support cryptographic acceleration.

Oracle Exadata X2-2 and X2-8 have the same CPUs in their storage nodes, but different CPUs in their compute nodes:

EXADATA MODEL	X2-2		X2-8	
NODE	ENCRYPT	DECRYPT	ENCRYPT	DECRYPT
Compute	Hardware acceleration enabled by patch 10080579 (Intel® X5670)	Hardware acceleration enabled by default (Intel® X5670)	Reduced hardware acceleration (~ 2x) through Nehalem technology in Intel® X7560	
Storage	n/a	Hardware acceleration enabled by default (Intel® L5640)	n/a	Hardware acceleration enabled by default (Intel® L5640)

Transparent Data Encryption and Applications

As part of Oracle's commitment to helping customers comply with regulations and insider threat concerns, Oracle Advanced Security Transparent Data Encryption has been certified with numerous applications:

TRANSPARENT DATA ENCRYPTION CERTIFIED WITH ORACLE AND 3RD PARTY APPLICATIONS:

TDE COLUMN ENCRYPTION	TDE TABLESPACE ENCRYPTION
Oracle E-Business Suite 11.5.9 and 12.x	Oracle E-Business Suite 11.5.10 and 12.x
Oracle PeopleSoft Enterprise 8.46+	Oracle PeopleSoft Enterprise 8.48+
Oracle Siebel CRM 7.7+	Oracle Siebel CRM 8.0
Oracle Internet Directory 10.1.4.2	Oracle JD Edwards EnterpriseOne
SAP 6.40 and later	SAP 6.40_EX2 and later
RETEK Sales Audit	
iFLEX FlexCube 10.0	

Oracle RMAN Encryption

Encrypting backups protects data should the backup media fall into the wrong hands or be lost during transit. It is recommended to encrypt database backups created with Oracle RMAN whether the data in the source database is encrypted or not (that includes the SYSTEM and SYSAUX tablespaces which cannot be encrypted by TDE). If TDE is used in the source database, RMAN can be instructed to use the TDE master encryption key of the source database; this is recommended when the backup is to be restored back to the same database. Alternatively, RMAN backups can be encrypted using a passphrase; this passphrase can easily be shared with the receiving site to decrypt the data upon restore. Additionally, TDE master encryption key **and** passphrase can be used at the same time, providing a maximum of security and flexibility. When TDE tablespace encryption is used in the source database, RMAN can also compress encrypted backups; data from the encrypted tablespace is decrypted, compressed, and re-encrypted. Encrypted application table columns are treated as if they are not encrypted, resulting in a reduced average compression ratio.

Oracle recommends backing up the Oracle Advanced Security TDE Wallet on separate media away from the encrypted backup, especially when an 'auto-open' wallet is used.

Oracle Data Pump Encryption

By default data exported from an Oracle Database using the Oracle Data Pump utility will be exported in clear text. Oracle Data Pump can be instructed to create encrypted and compressed export files with TDE. The Oracle Advanced Security TDE master key or a pass phrase, or both, can be used to encrypt the export file.

Oracle Advanced Security Encryption Key Management

Transparent Data Encryption uses a 2-tier key architecture for flexible and non-intrusive key rotation and least operational and performance impact: Each application table with at least one encrypted column has its own *table key*, which is applied to all encrypted columns in that table. Equally, each encrypted tablespace has its own *tablespace key*. Table keys are stored in the data dictionary of the database, while tablespace keys are stored in the header of the tablespace and additionally, the header of each underlying OS file that makes up the tablespace. Each of these keys is encrypted with the TDE master encryption key, which is stored outside of the database in an external security module: either the Oracle Wallet (a PKCS#12 formatted file that is encrypted using a passphrase supplied either by the designated security administrator or DBA during setup), or a Hardware Security Module (HSM) device for higher assurance, including those provided by Bull, Safenet, Thales and Utimaco. Oracle Advanced Security uses the industry standard PKCS#11 interface to communicate with the HSM devices. The table and tablespace keys can be AES (with 256, 192, or 128 bit key length), or 3DES168; the TDE master key is always an AES256 key.

Oracle Advanced Security Network Encryption

Oracle Advanced Security protects confidentiality and integrity of data travelling over the network using encryption and hashing, preventing data sniffing, data loss, replay and person-in-the-middle attacks. All communication with an Oracle Database can be encrypted with Oracle Advanced Security. Oracle Advanced Security provides both native encryption/data integrity algorithms and support for secure socket layer (SSL) to protect data over the network.

Oracle Advanced Security network encryption is completely transparent, easy to setup and requires no X.509 certificates. Oracle Advanced Security supports the following encryption algorithms:

- AES (256, 192 and 128 bits)
- 3DES (3 and 2 keys; 168 bits)
- RC4 (256 and 128 bits)
- SHA1

Secure Sockets Layer

SSL based encryption is available for businesses that have elected to provide public key infrastructure to their IT deployments. Oracle Advanced Security 10g introduced support for the TLS 1.0 protocol. Oracle Advanced Security provides AES cipher suites with the TLS 1.0 protocol starting in Oracle Database 10g.

Oracle implements the SSL protocol for encryption of data exchanged between database clients and the database. This includes data in Oracle Net Services (formerly known as Net8), LDAP,

thick (type 2) and thin (type 4) JDBC, and IIOP format. SSL encryption provides users with an alternative to Oracle Advanced Security native encryption.

In a three-tier system, SSL support in the database means that data exchanged between the middle tier and the database can be encrypted using SSL. Oracle's implementation of SSL supports the three standard modes of authentication, including anonymous (Diffie-Hellman), server-only authentication using X.509 certificates, and mutual (client-server) authentication with X.509.

JDBC Security

JDBC is an industry-standard that provides a standard for connecting to a relational database from a Java program. Oracle implements two types of JDBC drivers: Thick JDBC drivers built on top of the C-based Oracle Net Services client, and thin (pure Java) JDBC drivers to support downloadable applets.

Since thick JDBC (type 2) uses the full Oracle Net Services communications stack on both client and server, it can take advantage of existing Oracle Advanced Security encryption and authentication mechanisms. Because the thin JDBC (type 4) driver is designed for use with downloadable applets used over the Internet, Oracle includes a 100% Java implementation of Oracle Advanced Security encryption, integrity and authentication for use with thin clients.

Configuring the network parameters for the server and/or client enables the network encryption/integrity function. Most businesses can therefore easily uptake this technology as there are no changes required in the application.

Oracle Advanced Security Strong Authentication

Oracle Advanced Security provides strong authentication solutions as an alternative to traditional password based authentication. Oracle Advanced Security supports Kerberos, PKI and RADIUS solutions. Oracle Advanced Security enables database users to achieve single sign-on to the Oracle database in Windows environments in conjunction with a Microsoft KDC. Database users can use their PKI credentials stored in smart cards or other hardware storage modules to authenticate to the Oracle database. This is especially useful for users as it provides roaming access to the database via client server applications. Both Kerberos and PKI are supported with Oracle enterprise user security (EUS). EUS enables database users to be managed centrally in the Oracle Internet Directory or an existing enterprise LDAP repository in conjunction with Oracle Virtual Directory.

Kerberos Authentication

Oracle Advanced Security includes a Kerberos client that is compatible with a Kerberos v5 ticket that is issued by any MIT v5 compliant Kerberos server or Microsoft KDC. Businesses can continue to operate in a heterogeneous environment using Oracle Advanced Security's Kerberos

solution. Once an Oracle database is registered with a Kerberos Server and configured to support a Kerberos Service, enterprise users authenticate to the database directly, without authenticating to the database. Organizations that already use a Kerberos Server and Oracle Advanced Security's Kerberos adapter can migrate their external database users to the directory to benefit from centralized user management.

Oracle Database 11g Advanced Security Kerberos enhancements include support for principal names up to 2000 characters in length, and cross realm support allowing Kerberos principals in one realm to authenticate to Kerberos principals in another realm.

PKI Support

Oracle Advanced Security's SSL client can be used with industry standard X.509v3 certificates. Oracle Wallet Manager can be used to create certificate requests and manage other certificate management tasks. Additional command line utilities that assist in managing Certificate Revocation Lists (CRLs) and other Oracle Wallet operations are also available.

Certificate Revocation Lists published to an LDAP server, a file system or a URL are supported.

Oracle supports PKI integration and interoperability through:

- PKCS #7, #11 support
- Wallet storage in Oracle Internet Directory
- Multiple certificates per wallet
- Strong wallet encryption

Storing the wallet in a centralized LDAP-compliant directory supports user roaming, allowing users to access their credentials from multiple locations or devices, ensuring consistent and reliable user authentication, while providing centralized wallet management throughout the wallet life cycle.

Oracle Wallets support multiple certificates per wallet, including:

- S/MIME signing certificate
- S/MIME encryption certificate
- Code-signing certificate

RADIUS (Remote Authentication Dial-in User Service)

Oracle Advanced Security provides a Remote Authentication Dial-In User Service (RADIUS) client that allows the Oracle Database to respect the authentication and authorizations asserted by a RADIUS server. This feature is especially useful for businesses that are interested in two-factor authentication that establishes your identity based on what you know (password or PIN information) and what you have (the token card) provided by some token card manufacturers.

RADIUS 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 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.

Conclusion

Data encryption and strong authentication are key components of the defense-in-depth principle. Oracle has long been the leader in database security innovation and continues to develop new and exciting solutions to help customer's address rapidly emerging requirements around privacy and regulatory compliance. Retailers and financial institutions can use Oracle Advanced Security TDE to address PCI requirements while university and healthcare organizations can use TDE to address Health Insurance Portability and Accountability Act (HIPAA) requirements as well as safeguard social security numbers and other sensitive information. Oracle Advanced Security TDE protects sensitive data on disk drives and backup media from unauthorized access, helping reduce the impact of lost or stolen media. Oracle Advanced Security Network encryption plays an especially important role in safeguarding data in transit, preventing unauthorized sniffing of sensitive data traveling over the intranet. Strong authentication services such as Kerberos and PKI are gaining in popularity for high assurance user identification.

Oracle Advanced Security with
Oracle Database 11g Release 2
October 2010
Author: Peter Wahl, Paul Needham

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
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109