Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering
"Secure Coding: Developing Defensible Applications (DEV536)"
at http://software-security.sans.orghttp://software-security.sans.org/events/
Encryption is an important control used to protect private data, intellectual property and other sensitive data from external and internal attackers. With network perimeters dissolving, encryption is the one control that can prevent attackers from accessing sensitive data when other controls fail. Moreover, encryption of sensitive data is becoming a clear requirement for several compliance regulations.

Encryption traditionally applies to either data at rest or data in flight, and both crucial states of data are usually managed with different solutions. Oracle Advanced Security with Oracle Database 11g provides full-path encryption for database data while the data is on the network and at rest within database storage systems.

This paper is a review of Oracle Advanced Security encryption. It covers important product capabilities including network encryption for data in flight and Transparent Data Encryption (TDE) for data at rest. Although not covered in this paper, Oracle Advanced Security also provides support for strong user authentication to the database utilizing techniques such as Kerberos and Public Key Infrastructure (PKI).

Overall, Oracle Advanced Security encryption was easy to deploy in the testing environment, with nearly immediate usability. The solution provides built-in key management and common-sense configuration options such as encrypting in the database at the column or tablespace level, depending on business needs.
Oracle Advanced Security network encryption can be used with all of the currently supported versions of the Oracle database. Oracle Advanced Security TDE, however, was introduced for column-level encryption with Oracle Database 10g Release 2. Oracle Advanced Security TDE tablespace-level encryption is supported in Oracle Database 11g Release 1 and higher. For this reason, we selected an Oracle Database 11g database for testing.

For data-at-rest encryption, we used TDE tablespace encryption. Although Oracle Database 11g also supports column-level encryption, we reviewed tablespace encryption because that is Oracle’s default recommendation starting with Oracle Database 11g. For review purposes, we chose the command line interface to encrypt data; however, Oracle Enterprise Manager supports an easy-to-use graphical user interface.

For data-in-flight encryption, we used Oracle Advanced Security native network encryption for convenience, because it does not require PKI certificates. Note that Oracle fully supports standard SSL/TSL network encryption.
Oracle Advanced Security Network Encryption

To begin the review, we captured data that was not encrypted over the network, which is the default configuration for Oracle Databases that do not have Oracle Advanced Security protection. Next, we ran two SQL statements to query data from the `banking.customer` table and to create a user, as shown in Figure 1.

![Figure 1: Querying Data without Encryption](image)
The tcpdump utility on the database server captured the SQL statements from network traffic. The output shown in Figure 2 provides some of the data captured with tcpdump.

```
1640502230:1640502453(223) ack 1628512343 win 386 <nop,nop,timestamp 3088081 3047240>
 0x0000:  4500 0113 120a 4000 4006 fa02 c0a8 d643 E.....@.....C
 0x00010:  c0a8 d643 1ffe 05f1 61c8 13d6 6111 2057 ...C....a...a.W
 0x00020:  8018 0182 2ede 0000 0101 080a 002f 1ed1 ........../..
 0x00030:  002e 7f48 00df 0000 0600 0000 0000 1169 ..H........i
 0x00040:  1efe ffff ff01 0000 0002 0000 0003 5e1f ..........^.
 0x00050:  6180 0000 00000000feffff 5a00 0000 a........Z...
 0x00060:  feffff 0d00 0000 fefffffeffff ............
 0x00070:  0000 0000 0100 0000 0000000000000000 ............
 0x00080:  0000 00000000000000feffff 0000 0000 ............
 0x00090:  fefffffeffff 900d 3209 0000 0000 ........2....
 0x000a0:  0000 0000fefffffeffff 0000 0000 ............
 0x000b0:  0000 0000000000000000000000000000 ............
 0x000c0:  1e73 656c 6563 7420 2a20 6672 6f6d 2062  .select.*.from.b
 0x000d0:  616e 6b69 6e67 2e63 7573 746f 6d65 7201  anking.customer.
 0x000e0:  0000 0000000000000000000000000000 ............
 0x000f0:  0000 0000000000000000000000000000 ............
 0x00100:  0000 0000000000000000000000000000 ............
 0x00110:  0000 00
```

NOTE: Some data has been discarded due to length.

```
P 244:472(228) ack 1168 win 386 <nop,nop,timestamp 3094781 3088086>
 0x0000:  4500 0118 120a 4000 4006 f9f9 c0a8 d643 E.....@.....C
 0x0010:  c0a8 d643 1ffe 05f1 61c8 14ca 6111 246e ...C....a...a.$
 0x0020:  8018 0182 2ee3 0000 0101 080a 002f 38fd ........../8.
 0x0030:  002f 1ed6 00e4 0000 0600 0000 00001169 . ..........i
 0x0040:  21fe ffffe001 0000 0007 0000 0003 5e22 !...........
 0x0050:  2180 0000 00000000feffff 6900 0000 !...........
 0x0060:  feffff 0d00 0000 fefffffeffff ............
 0x0070:  0000 0000 0100 0000 0000000000000000 ............
 0x0080:  0000 00000000000000feffff 0000 0000 ............
 0x0090:  fefffffeffff 900d 3209 0000 0000 ........2....
 0x00a0:  0000 0000fefffffeffff 0000 0000 ............
 0x00b0:  0000 0000000000000000000000000000 ............
 0x00c0:  2363 7265 6174 2074 6573 7420 6964 656e  #create.user.tes
 0x00d0:  7469 6696 656e 7469 6696 6564 2062 7920 4identified.by.
 0x00e0:  7465 7374 0100 0000 0100 0000 0000000000test........
 0x00f0:  0000 0000000000000000000000000000000000 
 0x0100:  0500 0000 0000000000000000000000000000000000 
 0x0110:  0000 00000000000000
```

Figure 2: Unencrypted Data Captured with tcpdump
As you can see in Figure 2, the traffic was not encrypted, and the SQL statements were easy to read with just a small amount of additional capturing.

After verifying that the network data was being transmitted in the clear, it was time to conduct the same test with encryption enabled. To set up network encryption, you must first modify the `sqlnet.ora` file. In this case, we used the `SQLNET.CRYPTO_CHECKSUM_SERVER` and `SQLNET.ENCRYPTION_SERVER` parameters to specify that integrity (CHECKSUM) or encryption (ENCRYPTION) were used. You can set the parameters to REJECTED, ACCEPTED, REQUESTED or REQUIRED. We set the values to REQUIRED.

Once the checksum and encryption parameters were setup, we specified the algorithms to be used. In this case, we set the parameter `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER` to MD5 and the `SQLNET.ENCRYPTION_TYPES_SERVER` to DES40, RC4_40 encryption. Other encryption algorithms, including AES, 3DES and RSA RC4 could all be leveraged depending on needs. In production systems with defined security requirements, you would typically select options like AES128 and SHA-1 for improved cryptographic strength.

Once again, we ran the same SQL statements to query data from the `banking.customer` table and create a user. However, this time, no cleartext data was returned. All data was encrypted when the output was viewed. The output is provided in Figure 3.

```
0x0000: 4500 0118 a02b 4000 4006 6bdc c0a8 d643 E....+@. ........
0x0010: c0a8 d643 4791 05f1 a674 f349 a6aa ea24 ...CG....$.....
0x0020: 0818 0182 2ee3 0000 0101 080a 01ef a6dc ..........
0x0030: 01ef 4340 00e4 0000 0600 0000 0000be18 ..C@..........
0x0040: 2408 81b4 b031 c2e9 b166 21ea 23f4 bb05 S....fl....
0x0050: aeeb 645b b018 c0ad 6271 1dd3 de96 68fd ..[...bq....h.
0x0060: eb64 93fc a4a7 e507 9b71 1685 f7a0 d70e .d.......q......
0x0070: 459d 6c34 00e4 0000 0600 0000 0000be18 .C@..........
0x0080: 7922 72b7 ce1a 20cf 9fbe 9835 480b 7d8b y"r.......5H.}
0x0090: a07a e20f 03f9 0839 690b 40a7 8b5d beaa :z....9i@...a.
0x00a0: 9886 cf88 3b1a 9a5e e5fd da7e f080 02fa ........-
0x00b0: 7922 72b7 ce1a 20cf 9fbe 9835 480b 7d8b y"r.......5H.}
0x00c0: bfb7 7f0a 9a23 3438 2aad 86b3 759b a66f .....#48*...u..o
0x00d0: 51d9 3bb6 05b4 04d3 5ed5 d5b4 5e8d 6221 Q;.....^...^b!
0x00e0: f79d 459e f651 c57b e77e b060 97fd 5e2a ..E.Q{-`..^*
0x00f0: e425 d563 cfe4 53a2 c610 aeb3 5e2f 3a46 %.c...S...^/F
0x0100: e59d f510 f12b aca5 e55e 5b5d 0e65 8ce4 .....+^][].e..
```

**NOTE:** Some data has been discarded due to length.

Figure 3: Encrypted Data Captured with tcpdump

Network encryption was easy to setup, and we were able to obtain the benefits in short time. The fastest deployment of network encryption comes from a single configuration change to the `sqlnet.ora` file on the database server. This configuration drives the encryption decision from the server side, using only default settings that exist on the clients. Additional configuration options enable you to drive the encryption decision from the client side or from combined settings taken from both sides.
The second objective of this paper was to review how Oracle Advanced Security TDE encrypts data at rest. Oracle Advanced Security TDE is implemented in the database kernel, providing strong encryption for stored data. With Oracle Advanced Security TDE properly in place, malicious scans of database storage will not reveal encrypted information. From the standpoint of end users and applications, the presence of TDE is completely transparent because executed queries return real data as long as they are properly authorized by database access controls.

Oracle Advanced Security TDE also includes a command-line syntax to rotate the master key. The master key is always stored outside the database, whereas the table and tablespace keys are stored within the database. The master key can be stored in an external Oracle Wallet (a PKCS-12 compliant key management file) or optionally in a Hardware Security Module (HSM) from a certified vendor. When HSMs are used, the master key is exchanged over a standard PKCS-11 interface.

There are two encryption options with TDE: column-level encryption and tablespace encryption. In this review, we implemented tablespace encryption. In order to set up the encryption, we added the following to the \texttt{sqlnet.ora} file:

\begin{verbatim}
ENCRYPTION_WALLET_LOCATION=
  (SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/home/oracle/wallet))
\end{verbatim}

After modifying the \texttt{sqlnet.ora} file, our next step was to create the wallet. To do this, we issued the command “\texttt{alter system set encryption key identified by “abcdefg12#.”}” This created a wallet in the \texttt{/home/oracle/wallet} directory. Next, we ran another SQL command to make sure the wallet was in an open state and ready to encrypt data.
After enabling the database to use encryption, but before actually encrypting any data, we used a hex editor to view the data as it was currently stored in the data files. In its original, unencrypted state, the data in the `banking01.dbf` tablespace file was readable with the hex editor, as shown in Figure 4.

![Figure 4: Viewing Data Files in Their Unencrypted State](image-url)
The next step involved encrypting data in the `banking.customer` table by moving it into a new encrypted tablespace. To accomplish this, we issued the commands:

```
SQL> create tablespace bankingENC datafile
    
    '/u01/app/oracle/oradata/orcl/banking01ENC.dbf' size 1m ENCRYPTION
    
    default storage(ENCRYPT);

SQL> alter table banking.customer move tablespace bankingENC;
```

These commands created an encrypted tablespace and then moved the `banking.customer` table into it. To verify that the destination tablespace was encrypted, we executed a query command, as shown in Figure 5.

```
SQL> select tablespace_name, encrypted from dba_tablespaces;

<table>
<thead>
<tr>
<th>TABLESPACE_NAME</th>
<th>ENCRYPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>NO</td>
</tr>
<tr>
<td>SYSAUX</td>
<td>NO</td>
</tr>
<tr>
<td>UNDOTBS1</td>
<td>NO</td>
</tr>
<tr>
<td>TEMP</td>
<td>NO</td>
</tr>
<tr>
<td>USERS</td>
<td>NO</td>
</tr>
<tr>
<td>EXAMPLE</td>
<td>NO</td>
</tr>
<tr>
<td>BANKING</td>
<td>NO</td>
</tr>
<tr>
<td>BANKINGENC</td>
<td>YES</td>
</tr>
</tbody>
</table>

8 rows selected.
```

*Figure 5: Viewing the Encrypted Tablespace Attributes*
Next, we searched the encrypted tablespace file for the same data (TEMASEK) that was discovered in the unencrypted tablespace file. Because the data was now being encrypted, the hex editor was unable to find it, as illustrated in Figure 6.

Figure 6: Searching the New Tablespace File for Unencrypted Data

Alternatively, we could have encrypted specific table columns with TDE column-level encryption. Tablespace encryption can be useful when it is difficult to identify where all your sensitive data resides or when you need to encrypt a lot of data. Column-level encryption is useful when you only need to encrypt a few columns in known locations.

Overall, TDE encryption was easy to set up within the database. With just a few commands, we were able to implement database encryption while Oracle automatically setup, managed and stored the encryption keys for the application.
Conclusion

Today’s threats against databases and the private, intellectual property and other sensitive data stored in them call for additional, scalable protection. This includes encryption, the last line of defense to ward off attackers who may be using stolen operating system credentials, man-in-the-middle techniques such as sniffing, and other common attacks aimed at collecting critical database data.

The closest protection for data in transit and data at rest is encryption of the data itself. Such encryption ensures data in the database is not discoverable by unauthorized users and data sniffed on the network is rendered unreadable.

Oracle Advanced Security network encryption and Transparent Data Encryption for database data in motion and in storage has made it easy for users to meet business needs and compliance requirements.

Working closely with Oracle Database 11g, we found the tools to be intuitive to set up and we were able to start using them right away for both database encryption and network encryption. This ease of use eliminates one of the major barriers to organizations implementing encryption and provides immediate protection and compliance for sensitive database data.
**About the Author**

**Tanya Baccam** is a SANS senior instructor as well as a SANS courseware author. She is the current author for the SANS Security 509: Securing Oracle Databases course. Tanya works for Baccam Consulting, where she provides many security consulting services for clients, including system audits, vulnerability and risk assessments, database audits, and web application audits. Today much of her time is spent on the security of databases and applications within organizations. Tanya has also played an integral role in developing multiple business applications. She currently holds the CPA, GCFW, GCIH, CISSP, CISM, CISA and OCP DBA certifications.

---

SANS would like to thank its sponsor:

ORACLE®
# Upcoming SANS App Sec Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Northern Virginia 2015</td>
<td>Reston, VA</td>
<td>Mar 09, 2015 - Mar 14, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FL</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CA</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, Netherlands</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Seattle DEV522</td>
<td>Seattle, WA</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Capital City 2015</td>
<td>Washington, DC</td>
<td>Jul 06, 2015 - Jul 11, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London in the Summer</td>
<td>London, United Kingdom</td>
<td>Jul 13, 2015 - Jul 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago 2015</td>
<td>Chicago, IL</td>
<td>Aug 30, 2015 - Sep 04, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Gulf Region 2015</td>
<td>Dubai, United Arab Emirates</td>
<td>Oct 17, 2015 - Oct 29, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>