

2013



# ORACLE DATABASE VAULT AND TDE

Security issue - Oracle Database Vault and tablespace TDE not enough for hiding data from database administrators

## Environment description

- OS - Oracle Linux Server release 6.3
- Database – Oracle Database 11.2.0.3 EE with Database Vault and Transparent Data Encryption

## Experiment details

I want to prove, that ODV and TDE for tablespaces can be not enough for securing sensitive data from sysdba. In my example I will use HR schema and EMPLOYEES table for presentation purposes – let’s assume that my sensitive data are, for example, phone numbers of employees. I’ve created a realm that protects whole HR schema, so SYSDBA has no access to it.

```
SQL> select user
  2  from dual;

USER
-----
SYS

SQL> select count(1)
  2  from hr.jobs;
from hr.jobs
      *
ERROR at line 2:
ORA-01031: insufficient privileges
```

Additionally tablespace in which EMPLOYEES table resides is encrypted, so accessing datafile directly is useless.

```
SQL> select table_name, t.tablespace_name, ts.encrypted
  2  from dba_tables t, dba_tablespaces ts
  3  where t.tablespace_name=ts.tablespace_name
  4  and t.owner='HR'
  5  and t.table_name='EMPLOYEES';

TABLE_NAME          TABLESPACE_NAME    ENC
-----
EMPLOYEES            EMPLOYEES_AES128    YES
```

My Oracle Database is using AMM

```
SQL> sho parameters memory_target

NAME                TYPE        VALUE
-----
memory_target       big integer 1520M
SQL>
```

When I’m using AMM on Linux, memory is represented by files on /dev/shm device, which can be checked by ipcs and lsof commands

```
[root@rico ~]# ipcs

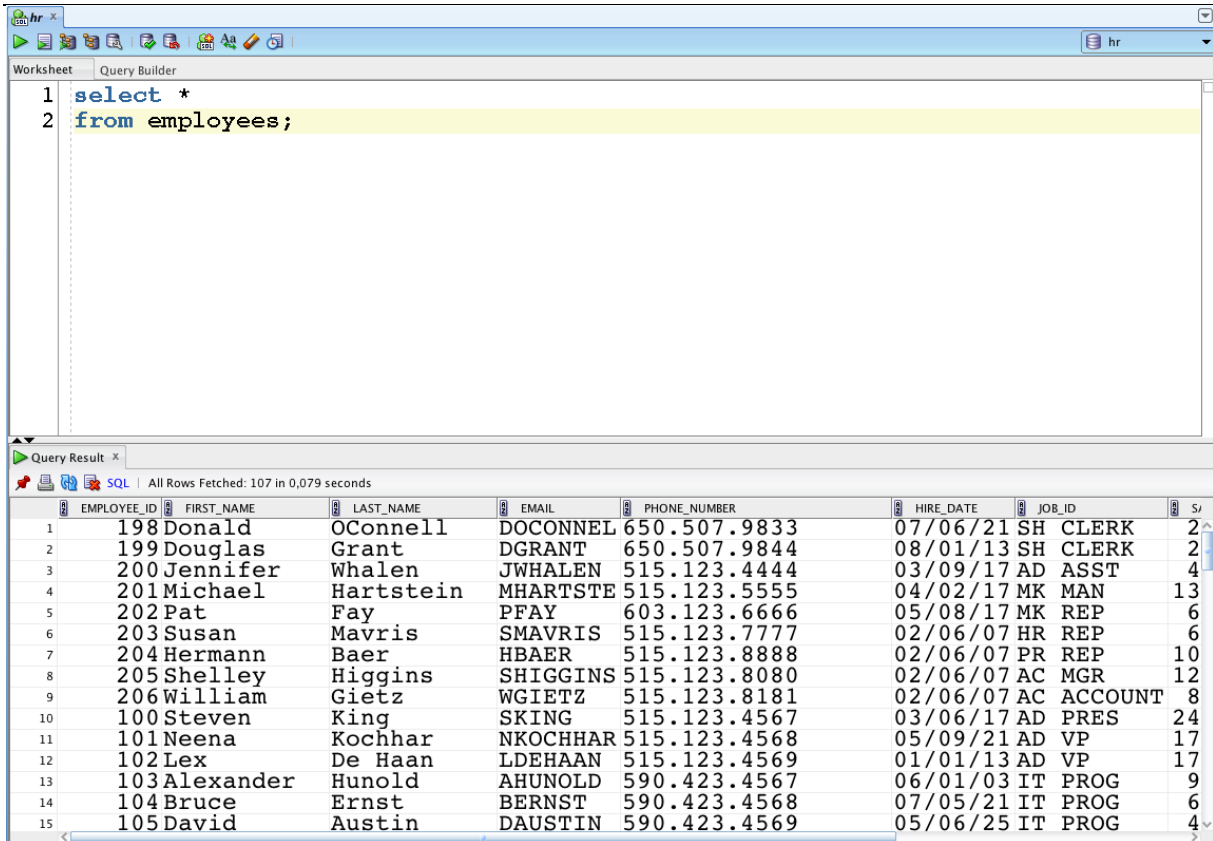
----- Shared Memory Segments -----
key      shmid   owner   perms   bytes   nattch   status
0x00000000 0       gdm     600     393216  2        dest
0x00000000 32769   gdm     600     393216  2        dest
0x00000000 65538   gdm     600     393216  2        dest
0x00000000 98307   gdm     600     393216  2        dest
0x00000000 131076  gdm     600     393216  2        dest
0x00000000 196613  oracle  640     4096    0
0x00000000 229382  oracle  640     4096    0
0xfa55c7d8 262151  oracle  640     4096    0
0x00000000 327688  oracle  640     4096    0
0x00000000 360457  oracle  640     4096    0
0x42e38fd0 393226  oracle  640     4096    0

----- Semaphore Arrays -----
key      semid   owner   perms   nsems
0x00000000 0       root    600     1
0x00000000 65537   root    600     1
0x496bed6c 196610  oracle  640     182
0x496bed6d 229379  oracle  640     182
0x496bed6e 262148  oracle  640     182
0x89a83438 393221  oracle  640     154

----- Message Queues -----
key      msqid   owner   perms   used-bytes   messages
```

```
[root@rico ~]# lsof | grep 393226
oracle 2632 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2634 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2636 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2640 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2642 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2644 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2646 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2648 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2650 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2652 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2654 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2656 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2658 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2660 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2662 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2664 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2666 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2668 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2672 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2674 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2680 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2732 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2743 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2748 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2766 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2778 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2797 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2799 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 2881 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 3309 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 3330 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 3433 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 3480 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
oracle 3482 oracle mem REG 0,17 16777216 21298 /dev/shm/ora_orcl_393226_0
```

Now let's issue SELECT statement on EMPLOYEES table as HR user from SQLDeveloper tool.



The screenshot shows the Oracle SQL Developer interface. The top pane displays a query: `select * from employees;`. The bottom pane shows the query results for the 'employees' table, listing columns: EMPLOYEE\_ID, FIRST\_NAME, LAST\_NAME, EMAIL, PHONE\_NUMBER, HIRE\_DATE, and JOB\_ID. The results include 15 rows of employee data.

EMPLOYEE_ID	FIRST_NAME	LAST_NAME	EMAIL	PHONE_NUMBER	HIRE_DATE	JOB_ID
198	Donald	OConnell	DOCONNEL	650.507.9833	07/06/21	SH_CLERK
199	Douglas	Grant	DGRANT	650.507.9844	08/01/13	SH_CLERK
200	Jennifer	Whalen	JWHALEN	515.123.4444	03/09/17	AD_ASST
201	Michael	Hartstein	MHARTSTE	515.123.5555	04/02/17	MK_MAN
202	Pat	Fay	PFAY	603.123.6666	05/08/17	MK_REP
203	Susan	Mavris	SMAVRIS	515.123.7777	02/06/07	HR_REP
204	Hermann	Baer	HBAER	515.123.8888	02/06/07	PR_REP
205	Shelley	Higgins	SHIGGINS	515.123.8080	02/06/07	AC_MGR
206	William	Gietz	WGIEZT	515.123.8181	02/06/07	AC_ACCOUNT
100	Steven	King	SKING	515.123.4567	03/06/17	AD PRES
101	Neena	Kochhar	NKOCHHAR	515.123.4568	05/09/21	AD VP
102	Lex	De Haan	LDEHAAN	515.123.4569	01/01/13	AD VP
103	Alexander	Hunold	AHUNOLD	590.423.4567	06/01/03	IT PROG
104	Bruce	Ernst	BERNST	590.423.4568	07/05/21	IT PROG
105	David	Austin	DAUSTIN	590.423.4569	05/06/25	IT PROG

After this query we should have blocks from EMPLOYEES segment copied into buffer cache – now lets see what we can do with it at OS level without any special privileges.

```
[oracle@rico ~]$ cd /dev/shm/
[oracle@rico shm]$ strings ora_orcl_* | egrep "[0-9]{3}\.[0-9]{3}\.[0-9]{4}$" | sort | uniq | tail -10
650.507.9833
650.507.9844
650.507.9876
650.507.9877
650.507.9878
650.507.9879
650.509.1876
650.509.2876
650.509.3876
650.509.4876
[oracle@rico shm]$
```

Looks familiar? ☺

## Conclusion

When Oracle database is using AMM on Linux (memory\_target parameter) ODV and encrypted tablespace is not enough for keeping sensitive data hidden from database administrator – if he knows what he is looking for...