PeteFinnigan.com Limited

create or replace function log_start[fv_path
return utl_file.file_type is
 lv_fptr utl_file.file_type:=null;
 lv_module varchar2[100]:='log_start';
begin   Oracle Security Expertise
 dbms_output.disable;

UKOUG Unix SIG,

Wolverhampton, May 20th 2009

The Right Method To Secure An Oracle Database

By

Pete Finnigan

Written Friday, 24th February 2009

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd
- Established Feb 2003
- http://www.petefinnigan.com
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases providing consultancy and training
- Database scanner software authors and vendor
- Author of Oracle security step-by-step book
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more)
- Member of the Oak Table Network

Quick Survey

- How many people here know "**where**" their key data is held?

- How many people here understand exactly "**who**" can see or "**modify**" key data?

- How many people here understand the true "**privilege model**" employed to protect "**key data**"?

Agenda

- Hardening by checklist
- Problems with checklists
- The right method
- Data flow
- Privilege/access assessment
- conclusions

Why We Need Security

- The target is often data not the DBA role
- The exploits we see on the internet work but stealing data is much more "real" and easy
- It is easy, not rocket science, no skill
- Real theft does not require complex techniques either
- What do you think happens in real life?
  - Exploits can be downloaded for free!
  - Stealing is easy because systems are open

21/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

5

Traditional Approach

- Hardening by checklist – good idea?

- A number of them available
  - SANS Step-by-step guide
  - SANS S.C.O.R.E.
  - CIS benchmark
  - DoD Stig
  - IT Governance book
  - Oracle's own checklist

Copyright (c) 2009
PeteFinnigan.com Limited

Problems With Checklists

- Not many lists exist
- Mostly from same initial source or very similar
- Some structure but not good enough
  - "tip based rather than method based"
- Doesn't focus on the data
- Difficult to implement for a large number of databases
- CIS for instance has 154 pages

Time "vs" Clever

- Time

  - Could spend man years on even a single database

  - Finding solutions for each issue is not as simple as applying what it says in the document

- Clever

  - Solutions are needed

  - Onion based approach

  - Basic hardening in parallel

Examples Of Problems

- Two examples:

  1) Check 3.0.2 in CIS states "all files in $ORACLE_HOME/bin directory must have privileges of 0755 or less – fine - but the solution states "chmod 0755 $ORACLE_HOME/bin/*" – good idea?

  2) Solutions are not as simple as indicated. For instance fixing a weak password should include, the password, management, hard coded passwords, audit, policy….

Checklists And PII Data

Some mention of data
BUT not focused

Copyright (c) 2009
PeteFinnigan.com Limited

Checklists And Special Data

No special data mentioned at all

The Right Method To Secure

- Start with "**the data**"

- Understand "**data flow**" and "**access**"

- Understand the problem of securing "**your data**"

- Hardening should be part of the solution **BUT** not **THE** solution

- Checklists do not mention "**your**" data

Complex But Simple Solutions

- Overarching solutions
- Remove all types of access from data
- Ensure only those who should see, can see the data
- Unfortunately its not simple as there are:
  - Many paths to the data
  - Many copies of data
  - Data stored or in transit that is accessible
  - Data copied outside of the database

Architecture

Users

DBA's

Feeds

Other databases

Power Users

backups

Data Feeds

Identify each type of person and a sample account for each

Data Access Models

Copyright (c) 2009
PeteFinnigan.com Limited

Data Access Is Not "Flat"

- Data model is not flat – remove the blinkers

- Access rights are also not flat

- Data is often replicated

  - In other tables – in interfaces – flexfields …

  - Indexes

  - Shared memory

  - Data files

  - Operating system

  - Many more…

Copyright (c) 2009
PeteFinnigan.com Limited

How / Who

- The data must be identified (found?)
- The access paths must be found
- The "people" – real people identified
- Map to database users
- Assess who can access data and how
- Only now can we hope to secure data

Securing Data

- We are going to investigate in depth the issues around a simple credit card table
- We need to
  - find the credit card table
  - Find duplicate copies
  - Assess who can access all
  - Other places the data exists
  - More…
- Even these issues are only the "*tip of the iceberg*" though!
- Lets dig deeper

Securing Data - 2

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl                _ □ X

who_can_access: Release 1.0.3.0.0 - Production on Fri Nov 28 16:25:13 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK          [USER_OBJECTS]: CREDIT_CARD
OWNER OF THE OBJECT TO CHECK           [USER]: ORABLOG
OUTPUT METHOD Screen/File                 [S]: S
FILE NAME FOR OUTPUT                [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:
EXCLUDE CERTAIN USERS                      [N]:
USER TO SKIP                          [TEST%]:

Checking object => ORABLOG.CREDIT_CARD
================================================================


Object type is => TABLE (TAB)
        Privilege => SELECT is granted to =>
        Role => PUBLIC (ADM = NO)

PL/SQL procedure successfully completed.


For updates please visit http://www.petefinnigan.com/t

SQL>
```

Look for the credit cards

This problem is often seen. The developers think that everyone accesses the data via their application.

The encrypted data could be stolen and cracked off line

Or decrypted on-line by any user

Copyright (c) 2009
PeteFinnigan.com Limited

Securing Data - 3

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl                    _ □ ×

Checking object => ORABLOG.ORABLOG_CRYPTO
========================================================

Object type is => PACKAGE (TAB)
        Privilege => EXECUTE is granted to =>
        Role => PUBLIC (ADM = NO)

PL/SQL procedure successfully completed.


For updates please visit http://www.petefinnigan.com/tools.

SQL> get dp
  1   select name,type,owner
  2   from dba_dependencies
  3   where referenced_name in ('DBMS_OBFUSCATION_TOOLKIT','DBMS_CRYPTO')
  4   and owner not in ('SYS','SYSMAN','FLOWS_03000')
  5* order by name desc
SQL> /

NAME                                TYPE              OWNER
--------------------------------    --------------    ---------------

WWV_FLOW_UTILITIES                  PACKAGE BODY      FLOWS_030000
WWV_FLOW_SECURITY                   PACKAGE BODY      FLOWS_030000
WWV_FLOW_ITEM                       PACKAGE BODY      FLOWS_030000
WWV_FLOW_DML                        PACKAGE BODY      FLOWS_030000
WWV_FLOW_COLLECTION                 PACKAGE BODY      FLOWS_030000
WWV_FLOW                            PACKAGE BODY      FLOWS_030000
WK_UTIL                             PACKAGE BODY      WKSYS
ORABLOG_CRYPTO                      PACKAGE BODY      ORABLOG
DBMS_OBFUSCATION_TOOLKIT            SYNONYM           PUBLIC
DBMS_CRYPTO                         SYNONYM           PUBLIC
BSLN                                PACKAGE BODY      DBSNMP

11 rows selected.

SQL> _
```

Test who can access the credit card crypto package

Again the same problem applies; there is a belief that no one will run this directly!

Securing Data - 4

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl              _ □ X
Wrote file afiedt.buf

  1   select name,type,owner
  2   from dba_dependencies
  3* where referenced_name='CREDIT_CARD'
SQL> /

NAME                              TYPE                 OWNER
-------------------------------   ------------------   ------------------

CC1                               VIEW                 ORABLOG

1 row selected.

SQL> edit
Wrote file afiedt.buf

  1   select name,type,owner
  2   from dba_dependencies
  3* where referenced_name='CC1'
SQL> /

NAME                              TYPE                 OWNER
-------------------------------   ------------------   ------------------

CCNAME                            VIEW                 ORABLOG

1 row selected.

SQL> edit
Wrote file afiedt.buf

  1   select name,type,owner
  2   from dba_dependencies
  3* where referenced_name='CCNAME'
SQL> /

no rows selected
```

Wow, there is not a single interface to our credit card data.

Each view now needs to be checked to see which users can access the credit card data via these views

Copyright (c) 2009
PeteFinnigan.com Limited

Securing Data - 5

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl          _ □ ×

SQL> select name,type,owner
  2    from dba_dependencies
  3    where referenced_name='ORABLOG_CRYPTO';

NAME                              TYPE                OWNER
--------------------------------  ------------------  -------------------------

ORABLOG_CRYPTO                    PACKAGE BODY        ORABLOG
CCDEC                             FUNCTION            ORABLOG
CCEN                              FUNCTION            ORABLOG

3 rows selected.

SQL>
```

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl          _ □ ×

who_can_access: Release 1.0.3.0.0 - Production on Fri Nov 28 16:50:36 2008
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF OBJECT TO CHECK         [USER_OBJECTS]: CCEN
OWNER OF THE OBJECT TO CHECK           [USER]: ORABLOG
OUTPUT METHOD Screen/File                 [S]: S
FILE NAME FOR OUTPUT                [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:
EXCLUDE CERTAIN USERS                     [N]:
USER TO SKIP                          [TEST%]:

Checking object => ORABLOG.CCEN
=============================================================================


Object type is => FUNCTION (TAB)
        Privilege => EXECUTE is granted to =>
        User => CC (ADM = NO)
```

Follow the same process as above

Test who can access the functions found

Securing Data - 6

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl

SQL> select owner,table_name from dba_tables
  2  where table_name like '%CREDIT%';

OWNER                               TABLE_NAME
----------------------------------  -------------------
ORABLOG                             CREDIT_CARD

1 row selected.

SQL> col owner for a10
SQL> col table_name for a30
SQL> col column_name for a5
SQL> select owner,table_name,column_name from dba_ta
  2  where column_name='PAN';

OWNER       TABLE_NAME                      COLUM
----------  ------------------------------  -----
ORABLOG     BIN$SFV0AmZ7LGngQAB/AQB5+w==$0  PAN
ORABLOG     BIN$SFV2LPPq6wHgQAB/AQB6GA==$0  PAN
ORABLOG     BIN$SFYmOpXjnWngQAB/AQAFSg==$0  PAN
ORABLOG     BIN$SFYqtq+wTp3gQAB/AQAGEA==$0  PAN
ORABLOG     BIN$SFYv3FNLr0DgQAB/AQAGQA==$0  PAN
ORABLOG     BIN$SFY2dIAeFVTgQAB/AQAGeA==$0  PAN
ORABLOG     BIN$SFY3HrgmcFrgQAB/AQAGgQ==$0  PAN
ORABLOG     BIN$SFY5dvNjURrgQAB/AQAGlw==$0  PAN
ORABLOG     BIN$SFY74g46F9fgQAB/AQAG8w==$0  PAN
ORABLOG     BIN$SFY/AtrNeRngQAB/AQAHGw==$0  PAN
ORABLOG     BIN$SFZJq3Itvb7gQAB/AQAHtw==$0  PAN
ORABLOG     BIN$SFZNmEOKfpjgQAB/AQAH+g==$0  PAN
ORABLOG     BIN$SFZSz8RAdAPgQAB/AQAIZg==$0  PAN
ORABLOG     BIN$SFZUh/pQIyfgQAB/AQAIew==$0  PAN
ORABLOG     BIN$SFZYZjtXUwngQAB/AQAIoQ==$0  PAN
ORABLOG     BIN$SFZZhezhGdPgQAB/AQAIsA==$0  PAN
ORABLOG     CREDIT_CARD                     PAN
ORABLOG     CC1                             PAN
IMPORTER    C23                             PAN

19 rows selected.
```

There are a number of issues here

The data is copied – we can check by looking at IMPORTER.PAN

The data is again duplicated in the recycle bin – this needs to be handled

Each table found has to be checked for hierarchy and access

If we could not find using simple ideas as here we would need to sample data or use specific algorithms

Securing Data - 7

Sweeping privileges are still dangerous for our data – o7_dictionary_accessibility prevents some hacks but does not stop sweeping data access
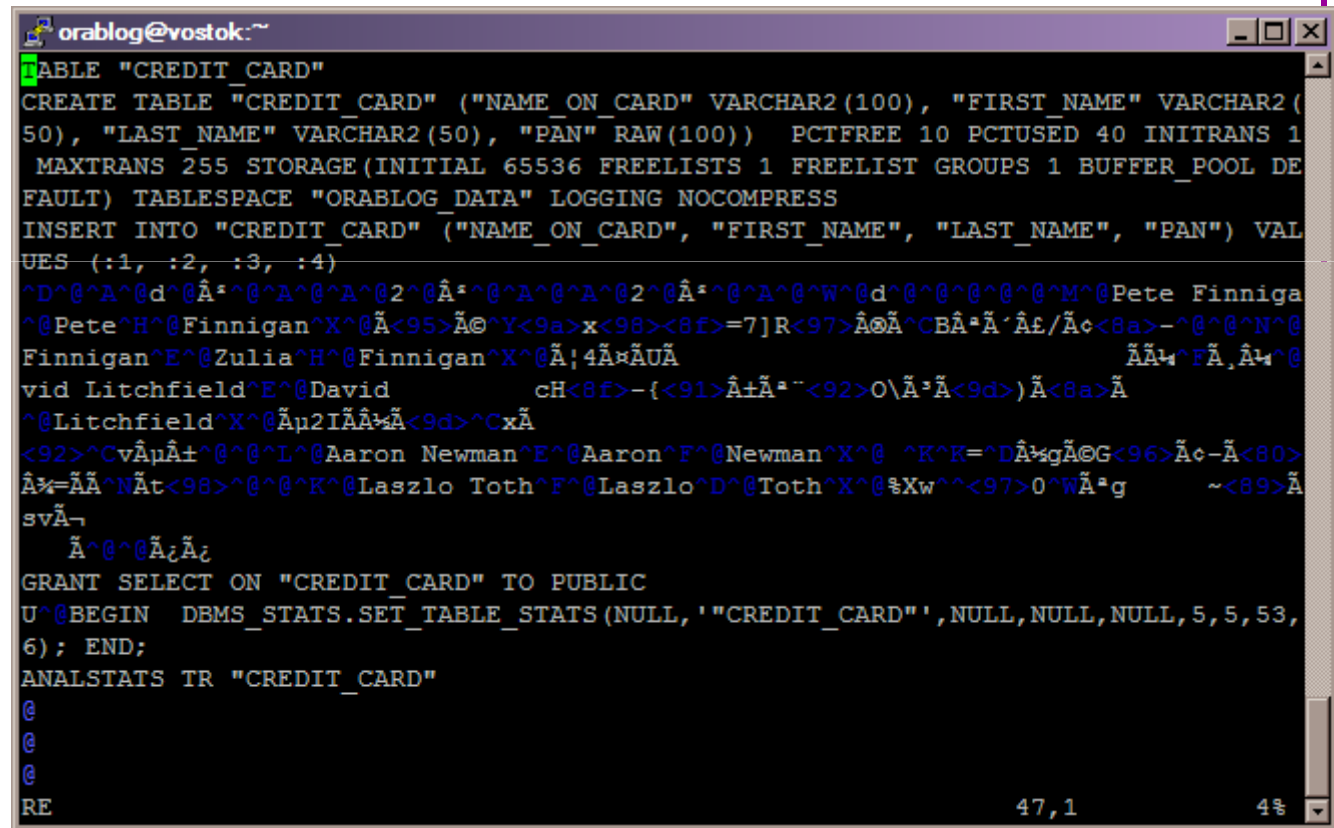
Remember there are other privileges; INSERT, UPDATE, DELETE…

Remember other privileges still that would allow data theft; TRIGGERS, EXECUTE PROCEDURE…

Copyright (c) 2009
PeteFinnigan.com Limited

Securing Data - 8

- The credit card data can be exposed via export, list files or any other OS / client based resource

Copyright (c) 2009
PeteFinnigan.com Limited

Securing Data - 9

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
SQL> get cc
  1    select sql_id,sql_text
  2    from v$sqltext
  3    where sql_id in (
  4    select sql_id
  5    from v$sqltext
  6    where upper(sql_text) like '%PAN%')
  7*   order by sql_id,piece
SQL> /

SQL_ID          SQL_TEXT
--------------- --------------------------------------------------------
2rn9a7dg9utp4   select sql_text from v$sqltext where upper(sql_text
2rn9a7dg9utp4   '
2ssufvzd2ukz9   select sql_id,sql_text from v$sqltext where sql_id
2ssufvzd2ukz9   ql_id from v$sqltext where upper(sql_text) like '%P
2ssufvzd2ukz9   y sql_id,piece
5bswhj9fzgba3   select name_on_card,orablog.orablog_crypto.decrypt(
5bswhj9fzgba3   blog.credit_card
6xn2s57zw4m5b   delete from opancillary$ where obj#=:1
7p7ssdnkvxwvt   SELECT occupant_name, occupant_desc, schema_name,
7p7ssdnkvxwvt     move_procedure, move_procedure_desc, space_usage_kbytes
7p7ssdnkvxwvt       FROM   gv$sysaux_occupants            WHERE  inst_id = USERENV(
7p7ssdnkvxwvt   'INSTANCE')
bp6du39yqhp7y   select sql_id,sql_text from v$sqltext where upper(sql_text) like
bp6du39yqhp7y    '%PAN%'
dxnnwy4497nh5   select name_on_card,orablog.orablog_crypto.decrypt(pan) from ora
dxnnwy4497nh5   blog.credit_card where orablog.orablog_crypto.decrypt(pan)='4049
dxnnwy4497nh5   990855468731'
f6cz4n8y72xdc   SELECT space_usage_kbytes   FROM   v$sysaux_occupants   WHERE occup
f6cz4n8y72xdc   ant_name = 'SQL_MANAGEMENT_BASE'
f7b9njbspa6g4   select name_on_card,orablog.orablog_crypto.decrypt(pan) from ora
f7b9njbspa6g4   blog.credit_card where orablog.orablog_crypto.decrypt(pan) like
f7b9njbspa6g4   '%4049%'

22 rows selected.

SQL>
```

The credit cards can also be exposed in shared memory and many other places

Privileges that allow access to dynamic data or meta-data must be reviewed

21/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

26

Securing Data - 10

- Securing data is not complex but we must take care of all access paths to the data
- We must consider the hierarchy
- We must consider sweeping privileges
- We must consider data leakage
- We must consider data replication
- There is more…unfortunately…
- In summary securing specific data ("***any data***") is first about knowing where that data is and who can access it and how it "***flows through the system***"

Users – The Opposite Problem

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1                    _ □ ×
SQL> set serveroutput on size 1000000
SQL> @cracker-v2.0.sql
cracker: Release 1.0.4.0.0 - Beta on Tue Nov 25 18:18:02 2008
Copyright (c) 2008 PeteFinnigan.com Limited. All rights reserved.

T Username                Password                CR FL STA
=================================================================
U "SYS"                   [ORACLE1           ] DI CR OP
U "SYSTEM"                [ORACLE1           ] DI CR OP
U "OUTLN"                 [OUTLN             ] DE CR EL
U "DIP"                   [DIP               ] DE CR EL
U "TSMSYS"                [TSMSYS            ] PU CR EL
U "ORACLE_OCM"            [ORACLE_OCM        ] PU CR EL
U "XDB"                   [CHANGE_ON_INSTALL ] DE CR EL
R "GLOBAL_AQ_USER_ROLE    [GL-EX {GLOBAL}    ] GE CR OP
U "DBSNMP"                [ORACLE1           ] DI CR OP
U "WMSYS"                 [WMSYS             ] DE CR EL
U "EXFSYS"                [EXFSYS            ] DE CR EL
U "CTXSYS"                [CHANGE_ON_INSTALL ] DE CR EL
U "XS$NULL"               [                  ] -- -- EL
U "ANONYMOUS"             [IMP {anonymous}   ] IM CR EL
R "SPATIAL_WFS_ADMIN"     [SPATIAL_WFS_ADMIN ] PU CR OP
U "ORDSYS"                [ORDSYS            ] DE CR EL
U "ORDPLUGINS"            [ORDPLUGINS        ] DE CR EL
U "SI_INFORMTN_SCHEMA"    [SI_INFORMTN_SCHEMA] DE CR EL
U "MDSYS"                 [MDSYS             ] DE CR EL
U "OLAPSYS"               [                  ] -- -- EL
U "MDDATA"                [MDDATA            ] DE CR EL
U "HR"                    [CHANGE_ON_INSTALL ] DE CR EL
U "SPATIAL_WFS_ADMIN_U    [SPATIAL_WFS_ADMIN_US] PU CR EL
R "WFS_USR_ROLE"          [WFS_USR_ROLE      ] PU CR OP
R "SPATIAL_CSW_ADMIN"     [SPATIAL_CSW_ADMIN ] PU CR OP
U "SPATIAL_CSW_ADMIN_U    [SPATIAL_CSW_ADMIN_US] PU CR EL
R "CSW_USR_ROLE"          [CSW_USR_ROLE      ] PU CR OP
U "WKSYS"                 [CHANGE_ON_INSTALL ] DE CR EL
U "WKPROXY"               [CHANGE_ON_INSTALL ] DE CR EL
U "WK_TEST"               [WK_TEST           ] DE CR EL
U "SYSMAN"                [ORACLE1           ] DI CR OP
U "MGMT_VIEW"             [                  ] -- -- OP
U "FLOWS_FILES"           [                  ] -- -- EL
U "APEX_PUBLIC_USER"      [                  ] -- -- EL
U "FLOWS_030000"          [                  ] -- -- EL
U "OWBSYS"                [OWBSYS            ] PU CR OP
R "OWB$CLIENT"            [S                 ] BF CR OP
R "OWB_DESIGNCENTER_VI    [S                 ] BF CR OP
U "SCOTT"                 [TIGER             ] DE CR EG
U "AB"                    [AB                ] PU CR OP
U "OE"                    [CHANGE_ON_INSTALL ] DE CR EL
U "IX"                    [CHANGE_ON_INSTALL ] DE CR EL
U "SH"                    [CHANGE_ON_INSTALL ] DE CR EL
U "PM"                    [CHANGE_ON_INSTALL ] DE CR EL
U "BI"                    [CHANGE_ON_INSTALL ] DE CR EL
U "PETE"                  [PETE              ] DE CR OP
U "BILL"                  [BILL              ] PU CR OP
U "A"                     [A                 ] PU CR OP
U "B"                     [B                 ] PU CR OP
U "C"                     [C                 ] PU CR OP
U "RES_TEST"              [RES_TEST          ] PU CR OP
U "XX"                    [123456            ] DI CR OP
U "ORASCAN"               [ORASCAN           ] PU CR OP
```

For this example run

INFO: Number of crack attempts = [61791]
INFO: Elapsed time = [4.36 Seconds]
INFO: Cracks per second = [14170]

53 out of 60 accounts cracked in 4.3 seconds

We are not trying to break in BUT trying to assess the "**real security level**"

See
http://www.petefinnigan.com/oracle_password_cracker.htm

Access Issue

User Types

```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1                          _|□|x|
SQL> set serveroutput on size 1000000
SQL> @cracker-v2.0.sql
cracker: Release 1.0.4.0.0 - Beta on Tue Nov 25 18:18:02 2008
Copyright (c) 2008 PeteFinnigan.com Limited. All rights reserved.

T Username                    Password               CR FL STA
**************************     **************         ****************

U "SYS"                       [ORACLE1           ] DI CR OP
U "SYSTEM"                     [ORACLE1           ] DI CR OP
U "OUTLN"                      [OUTLN             ] DE CR EL
U "DIP"                        [DIP               ] DE CR EL
U "TSMSYS"                     [TSMSYS            ] PU CR EL
U "ORACLE_OCM"                 [ORACLE_OCM        ] PU CR EL
U "XDB"                        [CHANGE_ON_INSTALL ] DE CR EL
R "GLOBAL_AQ_USER_ROLE         GL-EX (GLOBAL)     ] GE CR EL
U "DBSNMP"                     [ORACLE1           ] DI CR OP
U "WMSYS"                      [WMSYS             ] DE CR EL
U "EXFSYS"                     [EXFSYS            ] DE CR EL
U "CTXSYS"                     [CHANGE_ON_INSTALL ] DE CR EL
U "XS$NULL"                    [                  ] -- -- EL
U "ANONYMOUS"                  [IMP (anonymous)   ] IM CR EL
R "SPATIAL_WFS_ADMIN"          [SPATIAL_WFS_ADMIN ] PU CR OP
U "ORDSYS"                     [ORDSYS            ] DE CR EL
U "ORDPLUGINS"                 [ORDPLUGINS        ] DE CR EL
U "SI_INFORMTN_SCHEMA"         [SI_INFORMTN_SCHEMA] DE CR EL
U "MDSYS"                      [MDSYS             ] DE CR EL
U "OLAPSYS"                    [                  ] -- -- EL
U "MDDATA"                     [MDDATA            ] DE CR EL
U "MR"                         [CHANGE_ON_INSTALL ] DE CR EL
U "SPATIAL_WFS_ADMIN_U         [SPATIAL_WFS_ADMIN_US] PU CR EL
R "WFS_USR_ROLE"               [WFS_USR_ROLE      ] PU CR OP
R "SPATIAL_CSW_ADMIN"          [SPATIAL_CSW_ADMIN ] PU CR OP
U "SPATIAL_CSW_ADMIN_U         [SPATIAL_CSW_ADMIN_US] PU CR OP
R "CSW_USR_ROLE"               [CSW_USR_ROLE      ] PU CR OP
U "WKSYS"                      [CHANGE_ON_INSTALL ] DE CR EL
U "WKPROXY"                    [CHANGE_ON_INSTALL ] DE CR EL
U "WK_TEST"                    [WK_TEST           ] DE CR EL
U "SYSMAN"                     [ORACLE1           ] DI CR OP
U "MGMT_VIEW"                  [                  ] -- -- OP
U "FLOWS_FILES"                [                  ] -- -- EL
U "APEX_PUBLIC_USER"           [                  ] -- -- EL
U "FLOWS_030000"               [                  ] -- -- EL
U "OWBSYS"                     [OWBSYS            ] PU CR EL
R "OWB$CLIENT"                 [S                 ] BF CR OP
R "OWB_DESIGNCENTER_VI         [S                 ] BF CR OP
U "SCOTT"                      [TIGER             ] DE CR EG
U "AB"                         [AB                ] PU CR EL
U "OE"                         [CHANGE_ON_INSTALL ] DE CR EL
U "IX"                         [CHANGE_ON_INSTALL ] DE CR EL
U "SH"                         [CHANGE_ON_INSTALL ] DE CR EL
U "PM"                         [CHANGE_ON_INSTALL ] DE CR EL
U "BI"                         [CHANGE_ON_INSTALL ] DE CR EL
U "PETE"                       [PETE              ] DE CR OP
U "BILL"                       [BILL              ] PU CR OP
U "A"                          [A                 ] PU CR OP
U "B"                          [B                 ] PU CR OP
U "C"                          [C                 ] PU CR OP
U "RES_TEST"                   [RES_TEST          ] PU CR OP
U "XX"                         [123456            ] DI CR OP
U "ORASCAN"                    [ORASCAN           ] PU CR OP
```

- Shared passwords are a problem
- All privileged accounts have the same password
- This often implies that the same people do one job or multiple people share passwords
- If database links exist they possibly share the same passwords (check dump files)
- Assess not just what you see BUT the implications in terms of management and administration

Rounding Up

- A simple picture is built of all access to the key data

- All users are assessed and mapped to the data access

- Solutions are very specific but generally
  - Reduce default accounts
  - Reduce access to data
  - Remove duplicate privileges
  - Simplify privilege and access models
  - Generalise

Conclusions

- There are a few important lessons we must learn to secure data held in an Oracle database
  - We must secure the "**data**" not the software (quite obviously we MUST secure the software to achieve "**data**" security)
  - We must start with the "**data**" not the software
  - We must understand who/how/why/when "**data**" could be stolen
- Oracle security is complex though because we must consider "**where**" the "**data**" is and "**who**" can access it and "**how**"
- Often there are "**layers**" and "**duplication**"
- Careful detailed work is often needed

Copyright (c) 2009
PeteFinnigan.com Limited

Quick Survey – Again!

- How many people know "**where**" their key data is held?

- How many people understand exactly "**who**" can see or "**modify**" key data?

- How many people understand the true "**privilege model**" employed to protect "**key data**"?

Any Questions?

PeteFinnigan.com Limited

Oracle Security Expertise

```
create or replace function log_start(fv_path
return utl_file.file_type is
 lv_fptr utl_file.file_type:=null;
 lv_module varchar2(100):='log_start';
begin
 dbms_output.disable;
```

Contact - Pete Finnigan

PeteFinnigan.com Limited
9 Beech Grove, Acomb
York, YO26 5LD

Phone: +44 (0) 1904 791188
Mobile: +44 (0) 7742 114223
Email: pete@petefinnigan.com