

UKOUG Northern Server Tech Day,
York, April 28th 2009

The Right Method To Secure An Oracle Database

By
Pete Finnigan

Written Friday, 24th February 2009

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

1

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 and more)
- Member of the Oak Table Network



01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

2

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"**?

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

3

Agenda

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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

4

Why We Need Security

- The target is often data not the DBA role
- The exploits we see on the net 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

01/05/2009

Copyright (c) 2008
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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

6

Problems With Checklists

- Not many lists exist
- Mostly from same initial source
- Some structure but not good enough
- **Doesn't focus on the data**
- Difficult to implement for a large number of databases
- CIS for instance has 154 pages

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

7

Time / 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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

8

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....

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

9

Checklists And PII Data

| Item # | Configuration Item | Action / Recommended Parameters | Rationale/Remediation | Limit |
|--------|--------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| 5.25 | Encryption | Tablespace Encryption | Rationale: When a table contains a large number of columns of PII it can be beneficial to encrypt an entire tablespace rather than columns. Remediation: Use tablespace encryption. Audit: None | 4 |
| 5.26 | Radialkey | Verify and set permissions on radialkey file | Rationale: File permissions must be restricted to the owner of the Oracle database and its group. Ensure proper permissions are set on \$ORACLE_HOME/network/admin/psudm.asp Remediation: chmod 440 \$ORACLE_HOME Audit: ls -l \$ORACLE_HOME | 5 |
| 5.27 | Sqlnetora | \$ORACLE_HOME/network/admin/sqlnetora | Rationale: Oracle documentation is required for checking CDBs for client certificate authentication. Revoked certificates can cause an alert to be generated by the CDB database. | 5 |

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

10

Checklists And Special Data

| Item # | Configuration Item | Action / Recommended Parameters | Rationale/Remediation | Limit |
|--------|-------------------------------------|-------------------------------------------------------------------|-----------------------|-------|
| 1.1 | Microsoft Office Word 2007 | Verify and set permissions on Microsoft Office Word 2007 | | 1 |
| 1.2 | Microsoft Office Excel 2007 | Verify and set permissions on Microsoft Office Excel 2007 | | 1 |
| 1.3 | Microsoft Office PowerPoint 2007 | Verify and set permissions on Microsoft Office PowerPoint 2007 | | 1 |
| 1.4 | Microsoft Office Access 2007 | Verify and set permissions on Microsoft Office Access 2007 | | 1 |
| 1.5 | Microsoft Office Outlook 2007 | Verify and set permissions on Microsoft Office Outlook 2007 | | 1 |
| 1.6 | Microsoft Office OneNote 2007 | Verify and set permissions on Microsoft Office OneNote 2007 | | 1 |
| 1.7 | Microsoft Office Word 2003 | Verify and set permissions on Microsoft Office Word 2003 | | 1 |
| 1.8 | Microsoft Office Excel 2003 | Verify and set permissions on Microsoft Office Excel 2003 | | 1 |
| 1.9 | Microsoft Office PowerPoint 2003 | Verify and set permissions on Microsoft Office PowerPoint 2003 | | 1 |
| 1.10 | Microsoft Office Access 2003 | Verify and set permissions on Microsoft Office Access 2003 | | 1 |
| 1.11 | Microsoft Office Outlook 2003 | Verify and set permissions on Microsoft Office Outlook 2003 | | 1 |
| 1.12 | Microsoft Office OneNote 2003 | Verify and set permissions on Microsoft Office OneNote 2003 | | 1 |
| 1.13 | Microsoft Office Word 2000 | Verify and set permissions on Microsoft Office Word 2000 | | 1 |
| 1.14 | Microsoft Office Excel 2000 | Verify and set permissions on Microsoft Office Excel 2000 | | 1 |
| 1.15 | Microsoft Office PowerPoint 2000 | Verify and set permissions on Microsoft Office PowerPoint 2000 | | 1 |
| 1.16 | Microsoft Office Access 2000 | Verify and set permissions on Microsoft Office Access 2000 | | 1 |
| 1.17 | Microsoft Office Outlook 2000 | Verify and set permissions on Microsoft Office Outlook 2000 | | 1 |
| 1.18 | Microsoft Office OneNote 2000 | Verify and set permissions on Microsoft Office OneNote 2000 | | 1 |
| 1.19 | Microsoft Office Word 97-2003 | Verify and set permissions on Microsoft Office Word 97-2003 | | 1 |
| 1.20 | Microsoft Office Excel 97-2003 | Verify and set permissions on Microsoft Office Excel 97-2003 | | 1 |
| 1.21 | Microsoft Office PowerPoint 97-2003 | Verify and set permissions on Microsoft Office PowerPoint 97-2003 | | 1 |
| 1.22 | Microsoft Office Access 97-2003 | Verify and set permissions on Microsoft Office Access 97-2003 | | 1 |
| 1.23 | Microsoft Office Outlook 97-2003 | Verify and set permissions on Microsoft Office Outlook 97-2003 | | 1 |
| 1.24 | Microsoft Office OneNote 97-2003 | Verify and set permissions on Microsoft Office OneNote 97-2003 | | 1 |

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

11

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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

12

Complex But Simple Solutions

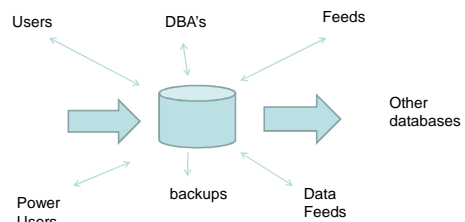
- Overarching solutions
- Remove all types of access from data
- Ensure only those who should, can see the data
- Unfortunately its not simple as there are
 - Many paths to the data
 - Many copies of data
 - Data stored or in transit that is accessible
 - Data copied outside of the database

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

13

Architecture



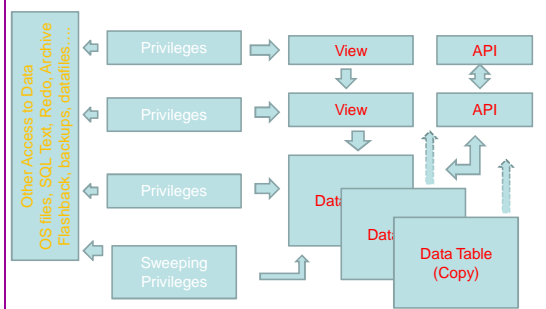
Identify each type of person and a sample account for each

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

14

Data Access Models



01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

15

Data Access Is Not "Flat"

- Data model is not flat
- 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...

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

16

How / Who

- The data must be identified
- The access paths 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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

17

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

01/05/2009

Copyright (c) 2008
PeteFinnigan.com Limited

18

Securing Data - 8

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

```

orablog@vnotok:~$ cat /dev/null > /dev/null
CREATE TABLE "CREDIT_CARD" ("NAME_ON_CARD" VARCHAR2(100), "FIRST_NAME" VARCHAR2(50), "LAST_NAME" VARCHAR2(50), "PAN" RAW(100)) PCTFREE 10 PCTUSED 40 INTRANS 1
MAXTRANS 255 STORAGE (INITIAL 65536 FREELISTS 1 FREELIST GROUPS 1 BUFFER_POOL DEFAULT) TABLESPACE "ORACLE_DATA" LOGGING NOCOMPRESSION
INSERT INTO "CREDIT_CARD" ("NAME_ON_CARD", "FIRST_NAME", "LAST_NAME", "PAN") VALUES (11, 12, 13, 14)
...
GRANT SELECT ON "CREDIT_CARD" TO PUBLIC
...

```

Securing Data - 9

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

```

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')
SQL> /
SQL_ID SQL_TEXT
-----
2m9a7d6g7atp4 select sql_text from v$sqltext where upper(sql_text)
2sufvcd2akb29 select sql_id,sql_text from v$sqltext where sql_id
2sufvcd2akb29 / sql_id,piece
2sufvcd2akb29 select name_on_card,orablog_cypto.decrypt(
2sufvcd2akb29 blog.credit_card
2sufvcd2akb29 delete from opsncillary2 where obj#=#
2sufvcd2akb29 SELECT occupant_name, occupant_desc, schema_name,
2sufvcd2akb29 name, procedure, more_procedure_desc, cpaec_usage_bytes
2sufvcd2akb29 FROM gv$sysaux_occupants WHERE inst_id = USERENV(
2sufvcd2akb29 'INSTANCE')
2sufvcd2akb29 select sql_id,sql_text from v$sqltext where upper(sql_text) like
2sufvcd2akb29 '>PAN';
2sufvcd2akb29 select name_on_card,orablog_cypto.decrypt(pan) from ora
2sufvcd2akb29 blog.credit_card where orablog_cypto.decrypt(pan)='>PAN'
2sufvcd2akb29 SELECT system_name_bytes FROM gv$sysaux_occupants WHERE occup
2sufvcd2akb29 ant_name = 'SQL_MANAGEMENT_BRIEF'
2sufvcd2akb29 select name_on_card,orablog_cypto.decrypt(pan) from ora
2sufvcd2akb29 blog.credit_card where orablog_cypto.decrypt(pan) like
2sufvcd2akb29 '>PAN';
22 rows selected.
SQL>

```

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@orcl
SQL> select * from user$;
NAME          USERNAME          SYSOPR  SYSADM  SYSINQ  SYSRDL  SYSBCK  SYSOPR  SYSADM  SYSINQ  SYSRDL  SYSBCK
-----          -----          -
SYS            SYS              YES      YES      YES      YES      YES
SYSOPER        SYSOPER          YES      YES      YES      YES      YES
SYSBACKUP      SYSBACKUP        YES      YES      YES      YES      YES
SYSDG           SYSDG            YES      YES      YES      YES      YES
SYSRAC          SYSRAC           YES      YES      YES      YES      YES
SYSKM           SYSKM             YES      YES      YES      YES      YES
SYSDEV          SYSDEV            YES      YES      YES      YES      YES
SYSDEV2         SYSDEV2           YES      YES      YES      YES      YES
SYSDEV3         SYSDEV3           YES      YES      YES      YES      YES
SYSDEV4         SYSDEV4           YES      YES      YES      YES      YES
SYSDEV5         SYSDEV5           YES      YES      YES      YES      YES
SYSDEV6         SYSDEV6           YES      YES      YES      YES      YES
SYSDEV7         SYSDEV7           YES      YES      YES      YES      YES
SYSDEV8         SYSDEV8           YES      YES      YES      YES      YES
SYSDEV9         SYSDEV9           YES      YES      YES      YES      YES
SYSDEV10        SYSDEV10          YES      YES      YES      YES      YES
SYSDEV11        SYSDEV11          YES      YES      YES      YES      YES
SYSDEV12        SYSDEV12          YES      YES      YES      YES      YES
SYSDEV13        SYSDEV13          YES      YES      YES      YES      YES
SYSDEV14        SYSDEV14          YES      YES      YES      YES      YES
SYSDEV15        SYSDEV15          YES      YES      YES      YES      YES
SYSDEV16        SYSDEV16          YES      YES      YES      YES      YES
SYSDEV17        SYSDEV17          YES      YES      YES      YES      YES
SYSDEV18        SYSDEV18          YES      YES      YES      YES      YES
SYSDEV19        SYSDEV19          YES      YES      YES      YES      YES
SYSDEV20        SYSDEV20          YES      YES      YES      YES      YES
SYSDEV21        SYSDEV21          YES      YES      YES      YES      YES
SYSDEV22        SYSDEV22          YES      YES      YES      YES      YES
SYSDEV23        SYSDEV23          YES      YES      YES      YES      YES
SYSDEV24        SYSDEV24          YES      YES      YES      YES      YES
SYSDEV25        SYSDEV25          YES      YES      YES      YES      YES
SYSDEV26        SYSDEV26          YES      YES      YES      YES      YES
SYSDEV27        SYSDEV27          YES      YES      YES      YES      YES
SYSDEV28        SYSDEV28          YES      YES      YES      YES      YES
SYSDEV29        SYSDEV29          YES      YES      YES      YES      YES
SYSDEV30        SYSDEV30          YES      YES      YES      YES      YES
SYSDEV31        SYSDEV31          YES      YES      YES      YES      YES
SYSDEV32        SYSDEV32          YES      YES      YES      YES      YES
SYSDEV33        SYSDEV33          YES      YES      YES      YES      YES
SYSDEV34        SYSDEV34          YES      YES      YES      YES      YES
SYSDEV35        SYSDEV35          YES      YES      YES      YES      YES
SYSDEV36        SYSDEV36          YES      YES      YES      YES      YES
SYSDEV37        SYSDEV37          YES      YES      YES      YES      YES
SYSDEV38        SYSDEV38          YES      YES      YES      YES      YES
SYSDEV39        SYSDEV39          YES      YES      YES      YES      YES
SYSDEV40        SYSDEV40          YES      YES      YES      YES      YES
SYSDEV41        SYSDEV41          YES      YES      YES      YES      YES
SYSDEV42        SYSDEV42          YES      YES      YES      YES      YES
SYSDEV43        SYSDEV43          YES      YES      YES      YES      YES
SYSDEV44        SYSDEV44          YES      YES      YES      YES      YES
SYSDEV45        SYSDEV45          YES      YES      YES      YES      YES
SYSDEV46        SYSDEV46          YES      YES      YES      YES      YES
SYSDEV47        SYSDEV47          YES      YES      YES      YES      YES
SYSDEV48        SYSDEV48          YES      YES      YES      YES      YES
SYSDEV49        SYSDEV49          YES      YES      YES      YES      YES
SYSDEV50        SYSDEV50          YES      YES      YES      YES      YES
SYSDEV51        SYSDEV51          YES      YES      YES      YES      YES
SYSDEV52        SYSDEV52          YES      YES      YES      YES      YES
SYSDEV53        SYSDEV53          YES      YES      YES      YES      YES
SYSDEV54        SYSDEV54          YES      YES      YES      YES      YES
SYSDEV55        SYSDEV55          YES      YES      YES      YES      YES
SYSDEV56        SYSDEV56          YES      YES      YES      YES      YES
SYSDEV57        SYSDEV57          YES      YES      YES      YES      YES
SYSDEV58        SYSDEV58          YES      YES      YES      YES      YES
SYSDEV59        SYSDEV59          YES      YES      YES      YES      YES
SYSDEV60        SYSDEV60          YES      YES      YES      YES      YES
SYSDEV61        SYSDEV61          YES      YES      YES      YES      YES
SYSDEV62        SYSDEV62          YES      YES      YES      YES      YES
SYSDEV63        SYSDEV63          YES      YES      YES      YES      YES
SYSDEV64        SYSDEV64          YES      YES      YES      YES      YES
SYSDEV65        SYSDEV65          YES      YES      YES      YES      YES
SYSDEV66        SYSDEV66          YES      YES      YES      YES      YES
SYSDEV67        SYSDEV67          YES      YES      YES      YES      YES
SYSDEV68        SYSDEV68          YES      YES      YES      YES      YES
SYSDEV69        SYSDEV69          YES      YES      YES      YES      YES
SYSDEV70        SYSDEV70          YES      YES      YES      YES      YES
SYSDEV71        SYSDEV71          YES      YES      YES      YES      YES
SYSDEV72        SYSDEV72          YES      YES      YES      YES      YES
SYSDEV73        SYSDEV73          YES      YES      YES      YES      YES
SYSDEV74        SYSDEV74          YES      YES      YES      YES      YES
SYSDEV75        SYSDEV75          YES      YES      YES      YES      YES
SYSDEV76        SYSDEV76          YES      YES      YES      YES      YES
SYSDEV77        SYSDEV77          YES      YES      YES      YES      YES
SYSDEV78        SYSDEV78          YES      YES      YES      YES      YES
SYSDEV79        SYSDEV79          YES      YES      YES      YES      YES
SYSDEV80        SYSDEV80          YES      YES      YES      YES      YES
SYSDEV81        SYSDEV81          YES      YES      YES      YES      YES
SYSDEV82        SYSDEV82          YES      YES      YES      YES      YES
SYSDEV83        SYSDEV83          YES      YES      YES      YES      YES
SYSDEV84        SYSDEV84          YES      YES      YES      YES      YES
SYSDEV85        SYSDEV85          YES      YES      YES      YES      YES
SYSDEV86        SYSDEV86          YES      YES      YES      YES      YES
SYSDEV87        SYSDEV87          YES      YES      YES      YES      YES
SYSDEV88        SYSDEV88          YES      YES      YES      YES      YES
SYSDEV89        SYSDEV89          YES      YES      YES      YES      YES
SYSDEV90        SYSDEV90          YES      YES      YES      YES      YES
SYSDEV91        SYSDEV91          YES      YES      YES      YES      YES
SYSDEV92        SYSDEV92          YES      YES      YES      YES      YES
SYSDEV93        SYSDEV93          YES      YES      YES      YES      YES
SYSDEV94        SYSDEV94          YES      YES      YES      YES      YES
SYSDEV95        SYSDEV95          YES      YES      YES      YES      YES
SYSDEV96        SYSDEV96          YES      YES      YES      YES      YES
SYSDEV97        SYSDEV97          YES      YES      YES      YES      YES
SYSDEV98        SYSDEV98          YES      YES      YES      YES      YES
SYSDEV99        SYSDEV99          YES      YES      YES      YES      YES
SYSDEV100       SYSDEV100         YES      YES      YES      YES      YES

```

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

User Types

```

C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
SQL> select * from user$;
NAME          USERNAME          SYSOPR  SYSADM  SYSINQ  SYSRDL  SYSBCK  SYSOPR  SYSADM  SYSINQ  SYSRDL  SYSBCK
-----          -----          -
SYS            SYS              YES      YES      YES      YES      YES
SYSOPER        SYSOPER          YES      YES      YES      YES      YES
SYSBACKUP      SYSBACKUP        YES      YES      YES      YES      YES
SYSDG           SYSDG            YES      YES      YES      YES      YES
SYSRAC          SYSRAC           YES      YES      YES      YES      YES
SYSKM           SYSKM             YES      YES      YES      YES      YES
SYSDEV          SYSDEV            YES      YES      YES      YES      YES
SYSDEV2         SYSDEV2           YES      YES      YES      YES      YES
SYSDEV3         SYSDEV3           YES      YES      YES      YES      YES
SYSDEV4         SYSDEV4           YES      YES      YES      YES      YES
SYSDEV5         SYSDEV5           YES      YES      YES      YES      YES
SYSDEV6         SYSDEV6           YES      YES      YES      YES      YES
SYSDEV7         SYSDEV7           YES      YES      YES      YES      YES
SYSDEV8         SYSDEV8           YES      YES      YES      YES      YES
SYSDEV9         SYSDEV9           YES      YES      YES      YES      YES
SYSDEV10        SYSDEV10          YES      YES      YES      YES      YES
SYSDEV11        SYSDEV11          YES      YES      YES      YES      YES
SYSDEV12        SYSDEV12          YES      YES      YES      YES      YES
SYSDEV13        SYSDEV13          YES      YES      YES      YES      YES
SYSDEV14        SYSDEV14          YES      YES      YES      YES      YES
SYSDEV15        SYSDEV15          YES      YES      YES      YES      YES
SYSDEV16        SYSDEV16          YES      YES      YES      YES      YES
SYSDEV17        SYSDEV17          YES      YES      YES      YES      YES
SYSDEV18        SYSDEV18          YES      YES      YES      YES      YES
SYSDEV19        SYSDEV19          YES      YES      YES      YES      YES
SYSDEV20        SYSDEV20          YES      YES      YES      YES      YES
SYSDEV21        SYSDEV21          YES      YES      YES      YES      YES
SYSDEV22        SYSDEV22          YES      YES      YES      YES      YES
SYSDEV23        SYSDEV23          YES      YES      YES      YES      YES
SYSDEV24        SYSDEV24          YES      YES      YES      YES      YES
SYSDEV25        SYSDEV25          YES      YES      YES      YES      YES
SYSDEV26        SYSDEV26          YES      YES      YES      YES      YES
SYSDEV27        SYSDEV27          YES      YES      YES      YES      YES
SYSDEV28        SYSDEV28          YES      YES      YES      YES      YES
SYSDEV29        SYSDEV29          YES      YES      YES      YES      YES
SYSDEV30        SYSDEV30          YES      YES      YES      YES      YES
SYSDEV31        SYSDEV31          YES      YES      YES      YES      YES
SYSDEV32        SYSDEV32          YES      YES      YES      YES      YES
SYSDEV33        SYSDEV33          YES      YES      YES      YES      YES
SYSDEV34        SYSDEV34          YES      YES      YES      YES      YES
SYSDEV35        SYSDEV35          YES      YES      YES      YES      YES
SYSDEV36        SYSDEV36          YES      YES      YES      YES      YES
SYSDEV37        SYSDEV37          YES      YES      YES      YES      YES
SYSDEV38        SYSDEV38          YES      YES      YES      YES      YES
SYSDEV39        SYSDEV39          YES      YES      YES      YES      YES
SYSDEV40        SYSDEV40          YES      YES      YES      YES      YES
SYSDEV41        SYSDEV41          YES      YES      YES      YES      YES
SYSDEV42        SYSDEV42          YES      YES      YES      YES      YES
SYSDEV43        SYSDEV43          YES      YES      YES      YES      YES
SYSDEV44        SYSDEV44          YES      YES      YES      YES      YES
SYSDEV45        SYSDEV45          YES      YES      YES      YES      YES
SYSDEV46        SYSDEV46          YES      YES      YES      YES      YES
SYSDEV47        SYSDEV47          YES      YES      YES      YES      YES
SYSDEV48        SYSDEV48          YES      YES      YES      YES      YES
SYSDEV49        SYSDEV49          YES      YES      YES      YES      YES
SYSDEV50        SYSDEV50          YES      YES      YES      YES      YES
SYSDEV51        SYSDEV51          YES      YES      YES      YES      YES
SYSDEV52        SYSDEV52          YES      YES      YES      YES      YES
SYSDEV53        SYSDEV53          YES      YES      YES      YES      YES
SYSDEV54        SYSDEV54          YES      YES      YES      YES      YES
SYSDEV55        SYSDEV55          YES      YES      YES      YES      YES
SYSDEV56        SYSDEV56          YES      YES      YES      YES      YES
SYSDEV57        SYSDEV57          YES      YES      YES      YES      YES
SYSDEV58        SYSDEV58          YES      YES      YES      YES      YES
SYSDEV59        SYSDEV59          YES      YES      YES      YES      YES
SYSDEV60        SYSDEV60          YES      YES      YES      YES      YES
SYSDEV61        SYSDEV61          YES      YES      YES      YES      YES
SYSDEV62        SYSDEV62          YES      YES      YES      YES      YES
SYSDEV63        SYSDEV63          YES      YES      YES      YES      YES
SYSDEV64        SYSDEV64          YES      YES      YES      YES      YES
SYSDEV65        SYSDEV65          YES      YES      YES      YES      YES
SYSDEV66        SYSDEV66          YES      YES      YES      YES      YES
SYSDEV67        SYSDEV67          YES      YES      YES      YES      YES
SYSDEV68        SYSDEV68          YES      YES      YES      YES      YES
SYSDEV69        SYSDEV69          YES      YES      YES      YES      YES
SYSDEV70        SYSDEV70          YES      YES      YES      YES      YES
SYSDEV71        SYSDEV71          YES      YES      YES      YES      YES
SYSDEV72        SYSDEV72          YES      YES      YES      YES      YES
SYSDEV73        SYSDEV73          YES      YES      YES      YES      YES
SYSDEV74        SYSDEV74          YES      YES      YES      YES      YES
SYSDEV75        SYSDEV75          YES      YES      YES      YES      YES
SYSDEV76        SYSDEV76          YES      YES      YES      YES      YES
SYSDEV77        SYSDEV77          YES      YES      YES      YES      YES
SYSDEV78        SYSDEV78          YES      YES      YES      YES      YES
SYSDEV79        SYSDEV79          YES      YES      YES      YES      YES
SYSDEV80        SYSDEV80          YES      YES      YES      YES      YES
SYSDEV81        SYSDEV81          YES      YES      YES      YES      YES
SYSDEV82        SYSDEV82          YES      YES      YES      YES      YES
SYSDEV83        SYSDEV83          YES      YES      YES      YES      YES
SYSDEV84        SYSDEV84          YES      YES      YES      YES      YES
SYSDEV85        SYSDEV85          YES      YES      YES      YES      YES
SYSDEV86        SYSDEV86          YES      YES      YES      YES      YES
SYSDEV87        SYSDEV87          YES      YES      YES      YES      YES
SYSDEV88        SYSDEV88          YES      YES      YES      YES      YES
SYSDEV89        SYSDEV89          YES      YES      YES      YES      YES
SYSDEV90        SYSDEV90          YES      YES      YES      YES      YES
SYSDEV91        SYSDEV91          YES      YES      YES      YES      YES
SYSDEV92        SYSDEV92          YES      YES      YES      YES      YES
SYSDEV93        SYSDEV93          YES      YES      YES      YES      YES
SYSDEV94        SYSDEV94          YES      YES      YES      YES      YES
SYSDEV95        SYSDEV95          YES      YES      YES      YES      YES
SYSDEV96        SYSDEV96          YES      YES      YES      YES      YES
SYSDEV97        SYSDEV97          YES      YES      YES      YES      YES
SYSDEV98        SYSDEV98          YES      YES      YES      YES      YES
SYSDEV99        SYSDEV99          YES      YES      YES      YES      YES
SYSDEV100       SYSDEV100         YES      YES      YES      YES      YES

```

- 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

01/05/2009

Copyright (c) 2008
PeteFinnigan.com Limited

31

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"**?

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

32

PeteFinnigan.com Limited

create or replace function log_error_path
return varchar2 as
begin
return 'PeteFinnigan.com Limited
Oracle Security Expertise
http://www.petefinnigan.com';
end;

Any Questions?

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

33

PeteFinnigan.com Limited

create or replace function log_error_path
return varchar2 as
begin
return 'PeteFinnigan.com Limited
Oracle Security Expertise
http://www.petefinnigan.com';
end;

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

01/05/2009

Copyright (c) 2009
PeteFinnigan.com Limited

34