PeteFinnigan.com Limited

Oracle Security Expertise

UKOUG Conference Birmingham,
November 30th 2009

The Right Method To Secure An Oracle Database

By

Pete Finnigan

Updated Monday, 12th October 2009

Why Am I Qualified To Speak

- PeteFinnigan.com Ltd, Est 2003.
- http://www.petefinnigan.com
- First "Oracle security" blog.
- Specialists in researching and securing Oracle databases providing consultancy and training Database scanner software authors and vendors.
- Author of Oracle security step-by-step book; co-author of Expert Oracle practices.
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, Finland and more).
- Member of the Oak Table Network.

Quick Quiz!

- 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 databases 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 to steal, 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

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

Problems With Checklists

- Not many checklists exist for Oracle databases
- Most are from same initial source or are very similar
- Some structure there but not good enough
  - "tip based rather than method based"
- Lists don't focus on securing the data
- Difficult to implement for a large number of databases
- CIS for instance has 158 pages

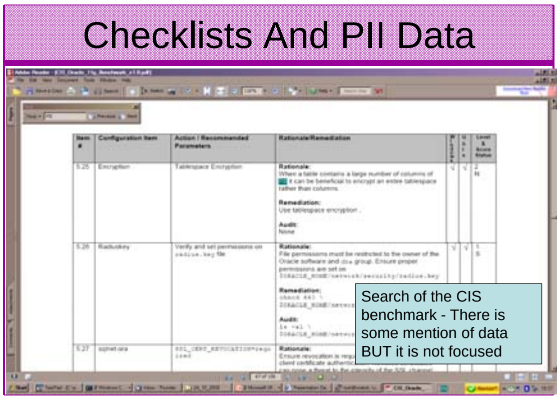
Time "vs" Clever

- Time solution
  - 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 solution
  - Technical solutions need to be specified
  - Onion based approach is good
  - 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/*" – is it a good idea?
  2) Solutions are not as simple as indicated. For instance fixing a weak password should also include, fix the password, management, hard coded passwords, audit, policy….

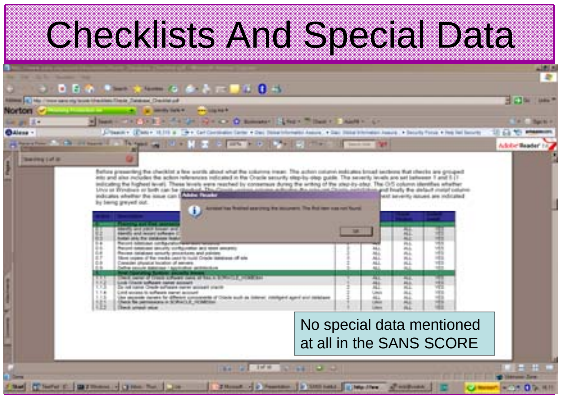
Checklists And PII Data



Item #	Configuration Item	Action / Recommended Parameters	Rationale/Remediation	[illegible]	[illegible]	Level & Score Status
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	√	√	2 N
5.26	Radiuskey	Verify and set permissions on radius.key file	**Rationale:** File permissions must be restricted to the owner of the Oracle software and dba group. Ensure proper permissions are set on $ORACLE_HOME/network/security/radius.key **Remediation:** chmod 440 \ $ORACLE_HOME/netw **Audit:** ls -al \ $ORACLE_HOME/netw	√	√	1 S
5.27	sqlnet.ora	SSL_CERT_REVOCATION=requ ired	**Rationale:** Ensure revocation is requ client certificate authentic			

Search of the CIS benchmark - There is some mention of data BUT it is not focused

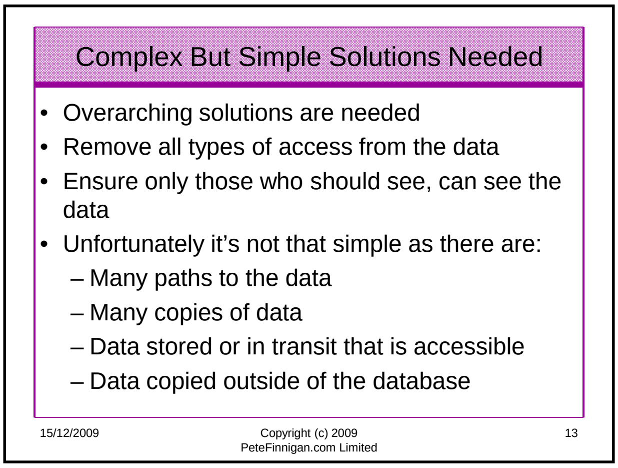
Checklists And Special Data



No special data mentioned at all in the SANS SCORE

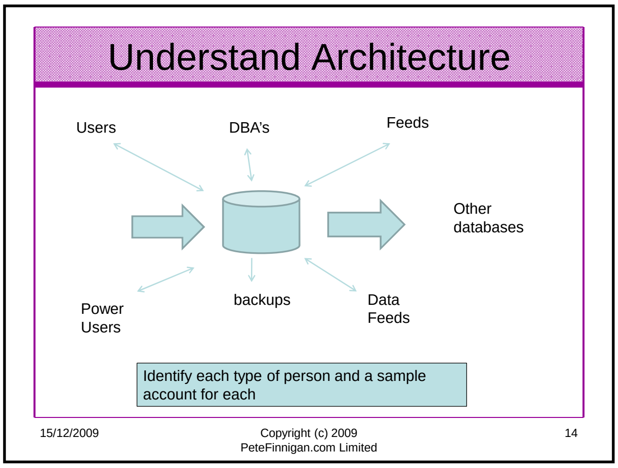
The Right Method To Secure

- 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



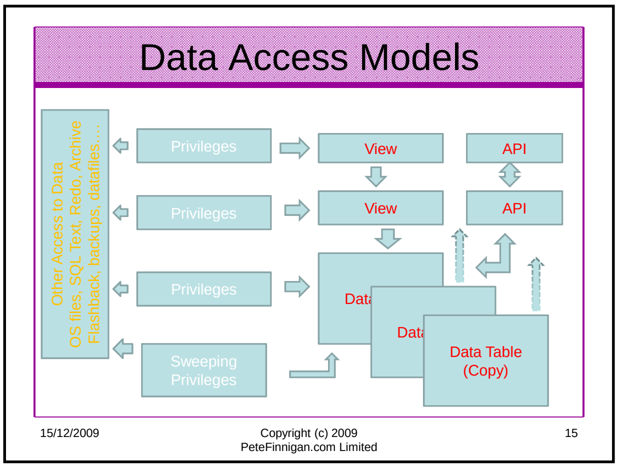
Complex But Simple Solutions Needed

- Overarching solutions are needed
- Remove all types of access from the data
- Ensure only those who should see, can see the data
- Unfortunately it’s not that 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

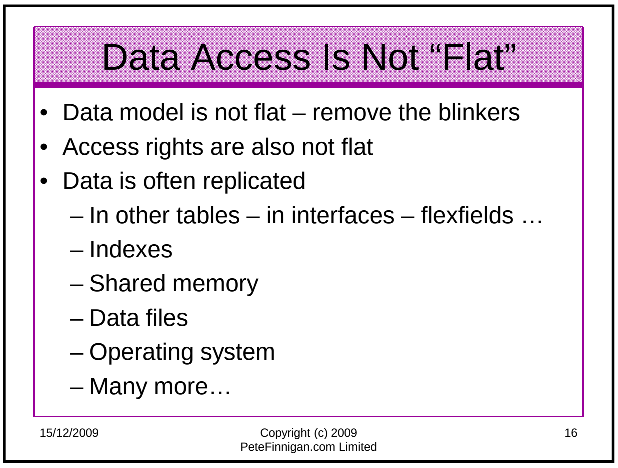


Understand Architecture

Identify each type of person and a sample account for each

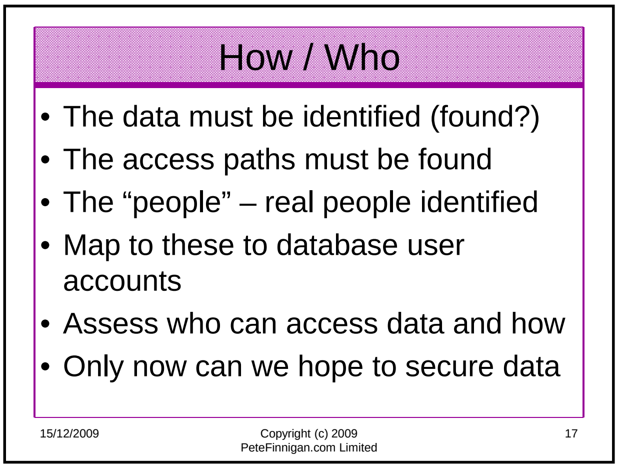


Data Access Models



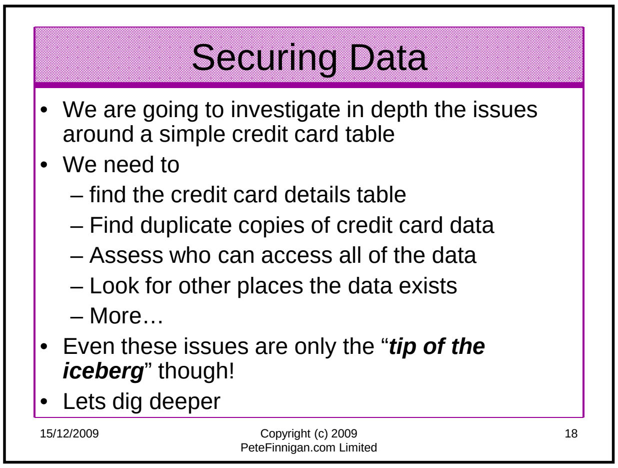
Data Access Is Not “Flat”

- 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…



How / Who

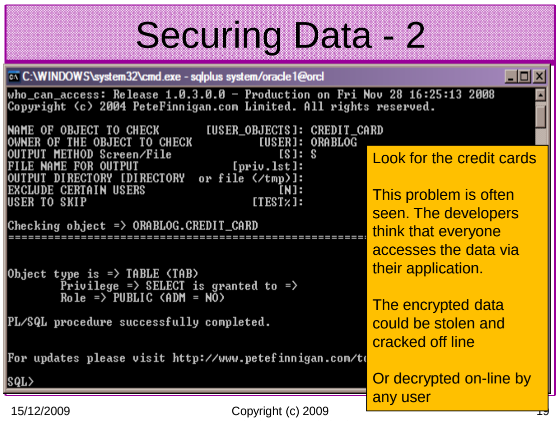
- The data must be identified (found?)
- The access paths must be found
- The “people” – real people identified
- Map to these to database user accounts
- Assess who can access data and how
- Only now can we hope to secure data



Securing Data

- We are going to investigate in depth the issues around a simple credit card table
- We need to
  - find the credit card details table
  - Find duplicate copies of credit card data
  - Assess who can access all of the data
  - Look for 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
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/to

SQL>
```

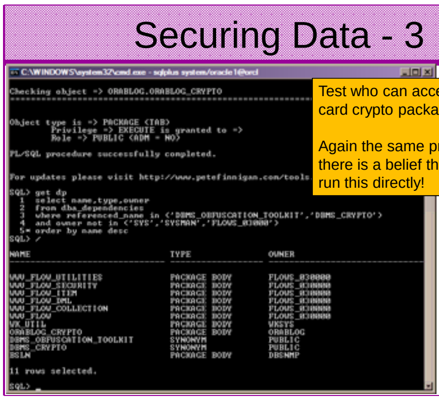
Look for the credit cards

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

Securing Data - 3

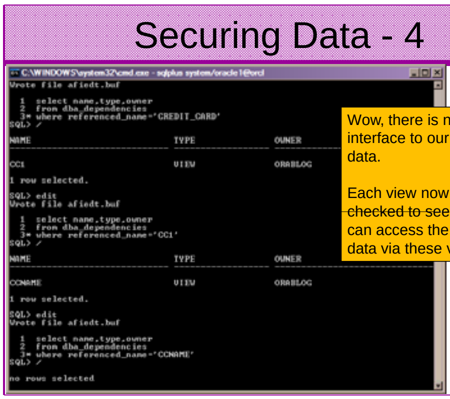


```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
Checking object => ORABLOG.ORABLOG_CRYPTO
=======================================================


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_030000')
  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

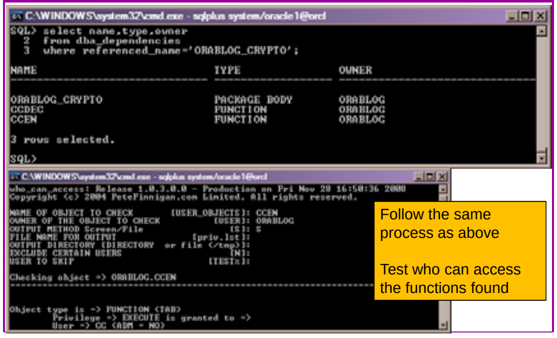


```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
Wrote file afiedt.buf

  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 se~~e which users can access the credit card data via these views

Securing Data - 5



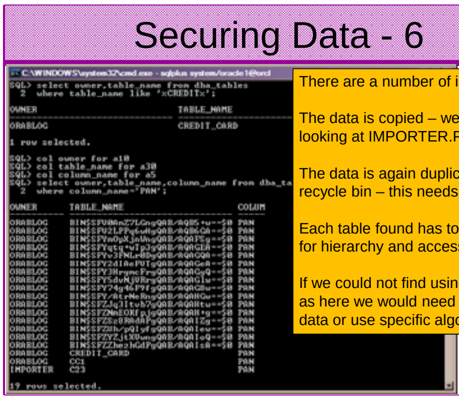
```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
SQL> select name,type,owner
  2  from dba_dependencies
  3  where referenced_name='ORABLOG_CRYPTO';

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$SFU0AmZ7LGngQAB/AQB5+w==$0 PAN
ORABLOG    BIN$SFU2LPPq6wHgQAB/AQB6GA==$0 PAN
ORABLOG    BIN$SFYm0pXjnWngQAB/AQAPSg==$0 PAN
ORABLOG    BIN$SFYqtq+wIpJgQAB/AQAGLA==$0 PAN
ORABLOG    BIN$SFYv3FNLr0DgQAB/AQAGQA==$0 PAN
ORABLOG    BIN$SFY2dIAePUTgQAB/AQAGeA==$0 PAN
ORABLOG    BIN$SFY3HrgmcFrgQAB/AQAGyQ==$0 PAN
ORABLOG    BIN$SFY5dvNjURrgQAB/AQAGlw==$0 PAN
ORABLOG    BIN$SFY74g46P9fgQAB/AQAGBw==$0 PAN
ORABLOG    BIN$SFY/AtrMeRngQAB/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/pQlyfgQAB/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

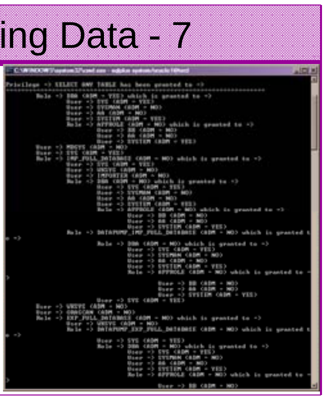
If we could not find using simple ideas as here we would need to sample data or use specific algorithms

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…

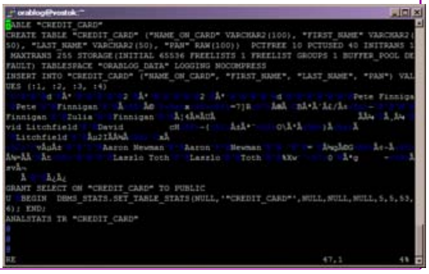
Remember other privileges still that would allow data theft; TRIGGERS, EXECUTE PROCEDURE…



```
C:\WINDOWS\system32\cmd.exe - sqlplus system/oracle1@orcl
Privilege => SELECT ANY TABLE has been granted to =>
=======================================================
        Role => DBA (ADM = YES) which is granted to =>
                User => SYS (ADM = YES)
                User => SYSMAN (ADM = NO)
                User => AA (ADM = NO)
                User => SYSTEM (ADM = YES)
                Role => APPROLE (ADM = NO) which is granted to =>
                        User => BB (ADM = NO)
                        User => AA (ADM = NO)
                        User => SYSTEM (ADM = YES)
        User => MDSYS (ADM = NO)
        User => SYS (ADM = YES)
        Role => IMP_FULL_DATABASE (ADM = NO) which is granted to =>
                User => SYS (ADM = YES)
                User => WKSYS (ADM = NO)
                User => IMPORTER (ADM = NO)
                Role => DBA (ADM = NO) which is granted to =>
                        User => SYS (ADM = YES)
                        User => SYSMAN (ADM = NO)
                        User => AA (ADM = NO)
                        User => SYSTEM (ADM = YES)
                        Role => APPROLE (ADM = NO) which is granted to =>
                                User => BB (ADM = NO)
                                User => AA (ADM = NO)
                                User => SYSTEM (ADM = YES)
                Role => DATAPUMP_IMP_FULL_DATABASE (ADM = NO) which is granted t
o =>
                        Role => DBA (ADM = NO) which is granted to =>
                                User => SYS (ADM = YES)
                                User => SYSMAN (ADM = NO)
                                User => AA (ADM = NO)
                                User => SYSTEM (ADM = YES)
                                Role => APPROLE (ADM = NO) which is granted to =
>
                                        User => BB (ADM = NO)
                                        User => AA (ADM = NO)
                                        User => SYSTEM (ADM = YES)
                        User => SYS (ADM = YES)
        User => WKSYS (ADM = NO)
        User => [illegible] (ADM = NO)
        Role => EXP_FULL_DATABASE (ADM = NO) which is granted to =>
                User => WKSYS (ADM = NO)
                Role => DATAPUMP_EXP_FULL_DATABASE (ADM = NO) which is granted t
o =>
                        User => SYS (ADM = YES)
                        Role => DBA (ADM = NO) which is granted to =>
                                User => SYS (ADM = YES)
                                User => SYSMAN (ADM = NO)
                                User => AA (ADM = NO)
                                User => SYSTEM (ADM = YES)
                                Role => APPROLE (ADM = NO) which is granted to =
>
                                        User => BB (ADM = NO)
```

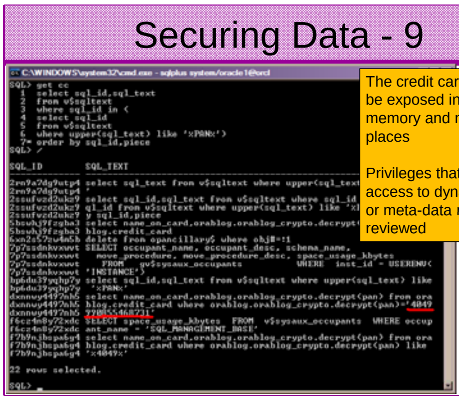
Securing Data - 8

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



```
ABLE "CREDIT_CARD"
CREATE TABLE "CREDIT_CARD" ("NAME_ON_CARD" VARCHAR2(100), "FIRST_NAME" VARCHAR2(
50), "LAST_NAME" VARCHAR2(50), "PAN" RAW(100))  PCTFREE 10 PCTUSED 40 INITRANS 1
 MAXTRANS 255 STORAGE(INITIAL 65536 FREELISTS 1 FREELIST GROUPS 1 BUFFER_POOL DE
FAULT) TABLESPACE "ORABLOG_DATA" LOGGING NOCOMPRESS
INSERT INTO "CREDIT_CARD" ("NAME_ON_CARD", "FIRST_NAME", "LAST_NAME", "PAN") VAL
UES (:1, :2, :3, :4)
        d  Å·        2  Å·        2  Å·        d             Pete Finniga
 Pete    Finnigan    Å    Å     ж        ~7]R     ÅмÅ  ñÅ·Å Å/Å     ~
Finnigan    Julia    Finnigan    Å;4Å»ÅûÅ                         ÅÅ  Å,Å
vid Litchfield    David          cH    ~(    ÅsÅ·     O\Å·Å     )Å     Å
 Litchfield    Åu2IÅÅ#Å        ñÅ
       vÅµÅ±        Aaron Newman    Aaron    Newman        ~  ÅwgÅDG    Å±-Å
ÅW-ÅÅ  Å±           Laszlo Toth    Laszlo    Toth    %Xw      0  Å·g     ~    Å
zvÅ~
  Å    Å¿Å¿
GRANT SELECT ON "CREDIT_CARD" TO PUBLIC
U  BEGIN  DBMS_STATS.SET_TABLE_STATS(NULL,'"CREDIT_CARD"',NULL,NULL,NULL,5,5,53,
6); END;
ANALSTATS TR "CREDIT_CARD"



RE                                                        47,1          4%
```

Securing Data - 9



```
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$sqltext where upper(sql_text) like '%
2ssufvzd2ukz9 y sql_id,piece
5bswhj9fzgba3 select name_on_card,orablog.orablog_crypto.decrypt(
5bswhj9fzgba3 blog.credit_card
6xn2s57zw4m5b delete from opancillary$ 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 770055468731'
f6cz4m8y72xdc SELECT space_usage_kbytes  FROM  v$sysaux_occupants  WHERE occup
f6cz4m8y72xdc 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>
```

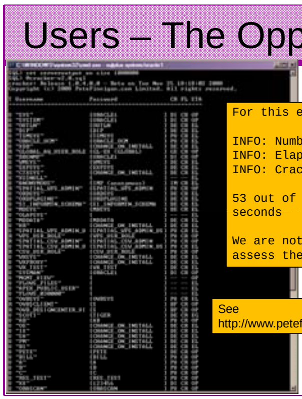
The credit cards can also be exposed in shared memory and many other places

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

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

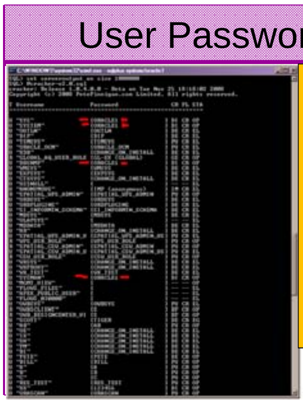


```
For this example run

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

This is called the “Access Issue”

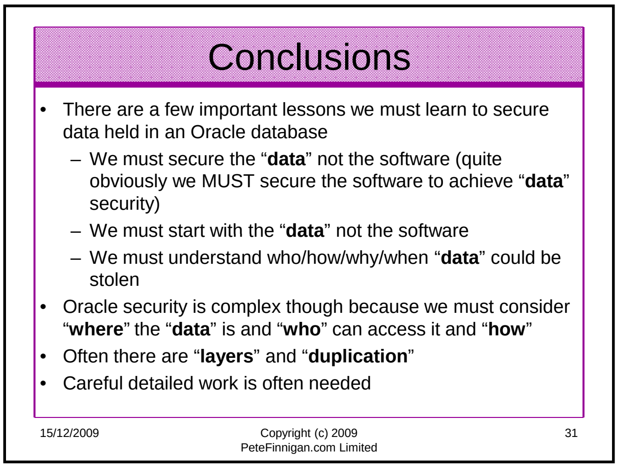
User Password Analysis



- 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 also the implications in terms of management and administration
- This is an example of just one issue

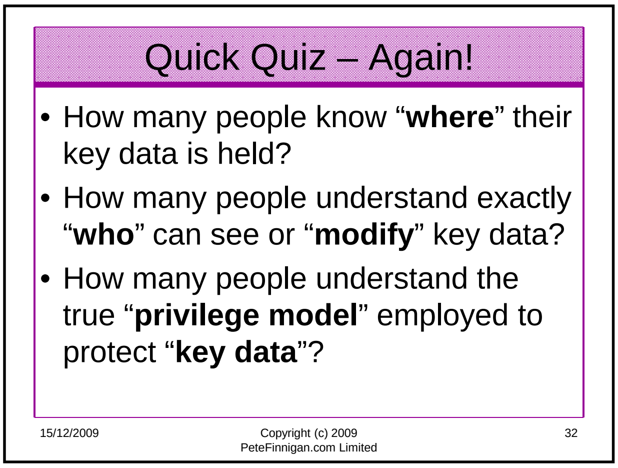
Rounding Up

- 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



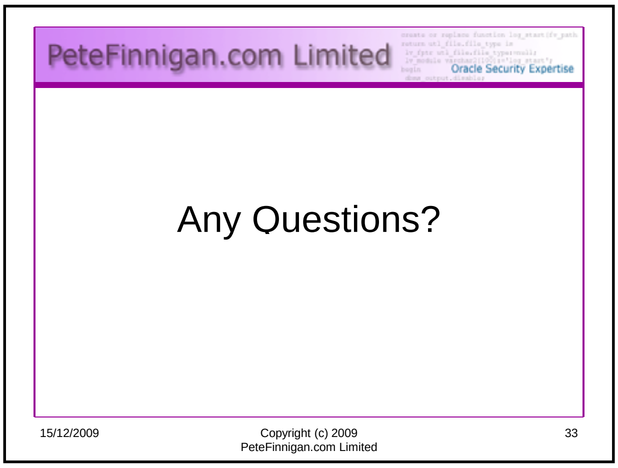
Conclusions

- 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



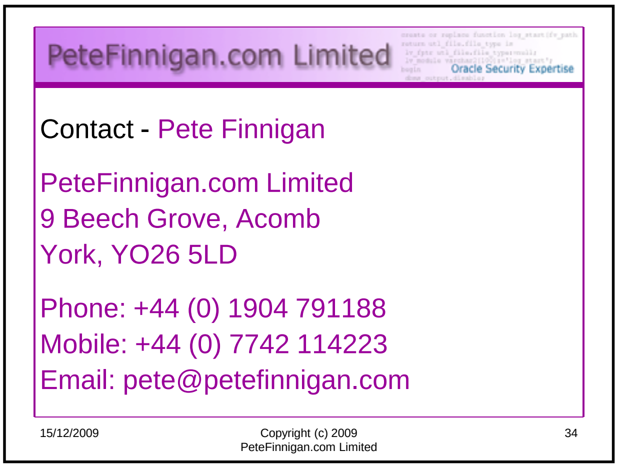
Quick Quiz – Again!

- 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**”?



PeteFinnigan.com Limited Oracle Security Expertise

Any Questions?



PeteFinnigan.com Limited Oracle Security Expertise

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