Database Link Security, Paul M. Wright, 19/11/2012.

Database links in Oracle suffer from a number of security issues, namely ..

1. DBLink password can be easily decrypted
2. Max SCN DoS threat
3. Anonymised Links between Prod/Dev and separate business unit subnets

In order to defend against these issues it would be useful to be able to ..

4. Identify incoming DBLinks
5. Forensically respond to an incident involving use of DBlinks

1. DBLink password can be easily decrypted

```
SQL> CREATE DATABASE LINK "TEST_LINK" CONNECT TO "DBLINK_ACCOUNT" IDENTIFIED BY MYPW USING
'(DESCRIPTION=(ADDRESS_LIST=(ADDRESS
=(PROTOCOL=TCP)(HOST=192.168.0.25)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=ORCL11)))';

Database link created.

SQL> select name, userid, passwordx from sys.link$ where name='TEST_LINK';
NAME
--------------------------------------------------------------------------------
USERID
------------------------------
PASSWORDX
--------------------------------------------------------------------------------
TEST_LINK
DBLINK_ACCOUNT
058CC531A7BBC08390C066B29CB2E26AF1

SQL> select name, userid, utl_raw.cast_to_varchar2(dbms_crypto.decrypt((substr(passwordx,19)),
4353, (substr(passwordx,3,16)))) from sys.link$ where name='TEST_LINK';

NAME
--------------------------------------------------------------------------------
USERID
------------------------------
PASSWORD
--------------------------------------------------------------------------------
TEST_LINK
DBLINK_ACCOUNT
MYPW

SQL> select * from v$version;
BANNER
--------------------------------------------------------------------------------
Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - Production
PL/SQL Release 11.2.0.2.0 - Production
CORE    11.2.0.2.0      Production
TNS for Linux: Version 11.2.0.2.0 - Production
NLSRTL Version 11.2.0.2.0 - Production
```

The above can be carried out by these users or holders of these roles/privileges on 11.2

- SYS
- SYSDBA
- DBA
- SYS WITHOUT SYSDBA
- SYSASM
- EXP_FULL_DATABASE
- DATAPUMP_EXP_FULL_DATABASE
- DATAPUMP_IMP_FULL_DATABASE

2. Max SCN DoS threat

As originally disclosed publicly by the Author back in 2009, the server SCN will be raised to that of the client SCN if it is higher, forcing a DoS when the SCN reaches the maximum. The risk of malicious threat from this issue is small compared to it's genuine maintenance impact in environments with high number of transactions. The main security risk from DBLinks comes from their unmonitored ability to cross security zones anonymously. For example Prod to Dev or between separate business unit subnets.

3. Anonymised Links between prod/dev and business subnets

DBLinks provide a method for an attacker to access a DB which anonymises their access and bypasses many of the logon controls present. Out of the box there is no method to stop incoming DBLinks. `GLOBAL_NAMES` can be set to `TRUE` but this only forces the source of a DBLink to check the domain name of a destination matches the source. What would be useful is a config setting to say *"don't allow DBLinks to enter my DB"*. Problem is, that it is difficult to identify incoming DBLinks , though not impossible as some believe.

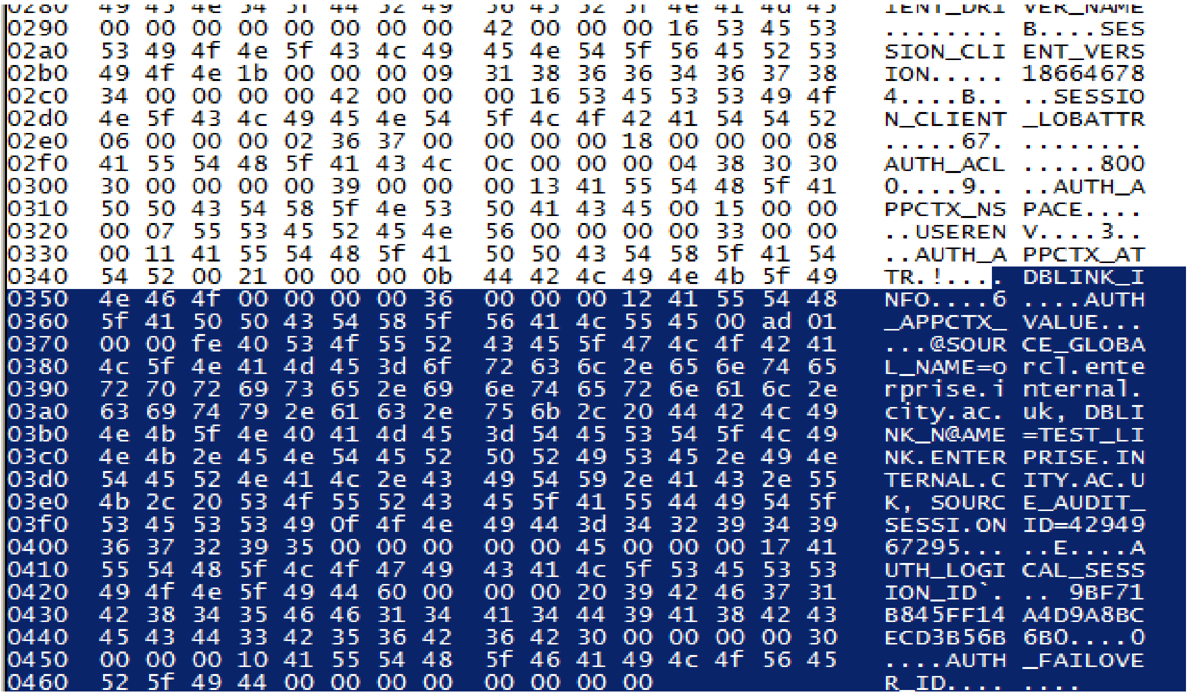
4. Identify incoming DBLinks

DBLinks are not specifically announced in `v$session` but on more recent versions of Oracle are recorded as DBLinks in `SYS.AUD$.COMMENT$TEXT` as demonstrated from 11.2.0.1 to 11.2.0.2 below:

```
select userid, terminal, comment$text from sys.aud$ where comment$text like 'DBLINK%';

USERID          NTIMESTAMP#            USERHOST   COMMENT$TEXT
------------   ------------------     -------    --------------
DBLINK_ACCOUNT     19-NOV-12 01.42.16.305194000  orlin    DBLINK_INFO: (SOURCE_GLOBAL_NAME=orcl.4294967295)
DBLINK_ACCOUNT     19-NOV-12 01.42.17.086395000  orlin    DBLINK_INFO: (SOURCE_GLOBAL_NAME=orcl.4294967295)
DBLINK_ACCOUNT     19-NOV-12 01.42.17.086856000  orlin    DBLINK_INFO: (SOURCE_GLOBAL_NAME=orcl.4294967295)
```

An immediate response to the above is.. *How does Oracle know they are incoming links?* and the answer to this is immediately viewable in a packet capture of a `SELECT` through a DB Link as shown in the next figure. Basically the client tells the DB that the source is a DBLink which is very handy.



```
0280  49 43 4e 54 5f 44 52 49  56 45 52 5f 4e 41 4d 45   IENT_DRI VER_NAME
0290  00 00 00 00 00 00 00 00  42 00 00 00 16 53 45 53   ........ B....SES
02a0  53 49 4f 4e 5f 43 4c 49  45 4e 54 5f 56 45 52 53   SION_CLI ENT_VERS
02b0  49 4f 4e 1b 00 00 00 09  31 38 36 36 34 36 37 38   ION..... 18664678
02c0  34 00 00 00 00 42 00 00  00 16 53 45 53 53 49 4f   4....B.. ..SESSIO
02d0  4e 5f 43 4c 49 45 4e 54  5f 4c 4f 42 41 54 54 52   N_CLIENT _LOBATTR
02e0  06 00 00 00 02 36 37 00  00 00 00 18 00 00 00 08   .....67. ........
02f0  41 55 54 48 5f 41 43 4c  0c 00 00 00 04 38 30 30   AUTH_ACL .....800
0300  30 00 00 00 00 39 00 00  00 13 41 55 54 48 5f 41   0....9.. ..AUTH_A
0310  50 50 43 54 58 5f 4e 53  50 41 43 45 00 15 00 00   PPCTX_NS PACE....
0320  00 07 55 53 45 52 45 4e  56 00 00 00 00 33 00 00   ..USEREN V....3..
0330  00 11 41 55 54 48 5f 41  50 50 43 54 58 5f 41 54   ..AUTH_A PPCTX_AT
0340  54 52 00 21 00 00 00 0b  44 42 4c 49 4e 4b 5f 49   TR.!.... DBLINK_I
0350  4e 46 4f 00 00 00 00 36  00 00 00 12 41 55 54 48   NFO....6 ....AUTH
0360  5f 41 50 50 43 54 58 5f  56 41 4c 55 45 00 ad 01   _APPCTX_ VALUE...
0370  00 00 fe 40 53 4f 55 52  43 45 5f 47 4c 4f 42 41   ...@SOUR CE_GLOBA
0380  4c 5f 4e 41 4d 45 3d 6f  72 63 6c 2e 65 6e 74 65   L_NAME=o rcl.ente
0390  72 70 72 69 73 65 2e 69  6e 74 65 72 6e 61 6c 2e   rprise.i nternal.
03a0  63 69 74 79 2e 61 63 2e  75 6b 2c 20 44 42 4c 49   city.ac. uk, DBLI
03b0  4e 4b 5f 4e 40 41 4d 45  3d 54 45 53 54 5f 4c 49   NK_N@AME =TEST_LI
03c0  4e 4b 2e 45 4e 54 45 52  50 52 49 53 45 2e 49 4e   NK.ENTER PRISE.IN
03d0  54 45 52 4e 41 4c 2e 43  49 54 59 2e 41 43 2e 55   TERNAL.C ITY.AC.U
03e0  4b 2c 20 53 4f 55 52 43  45 5f 41 55 44 49 54 5f   K, SOURC E_AUDIT_
03f0  53 45 53 53 49 0f 4f 4e  49 44 3d 34 32 39 34 39   SESSI.ON ID=42949
0400  36 37 32 39 35 00 00 00  00 00 45 00 00 00 17 41   67295... ..E....A
0410  55 54 48 5f 4c 4f 47 49  43 41 4c 5f 53 45 53 53   UTH_LOGI CAL_SESS
0420  49 4f 4e 5f 49 44 60 00  00 00 20 39 42 46 37 31   ION_ID`. .. 9BF71
0430  42 38 34 35 46 46 31 34  41 34 44 39 41 38 42 43   B845FF14 A4D9A8BC
0440  45 43 44 33 42 35 36 42  36 42 30 00 00 00 00 30   ECD3B56B 6B0....0
0450  00 00 00 10 41 55 54 48  5f 46 41 49 4c 4f 56 45   ....AUTH _FAILOVE
0460  52 5f 49 44 00 00 00 00  00 00 00 00               R_ID.... ....
```

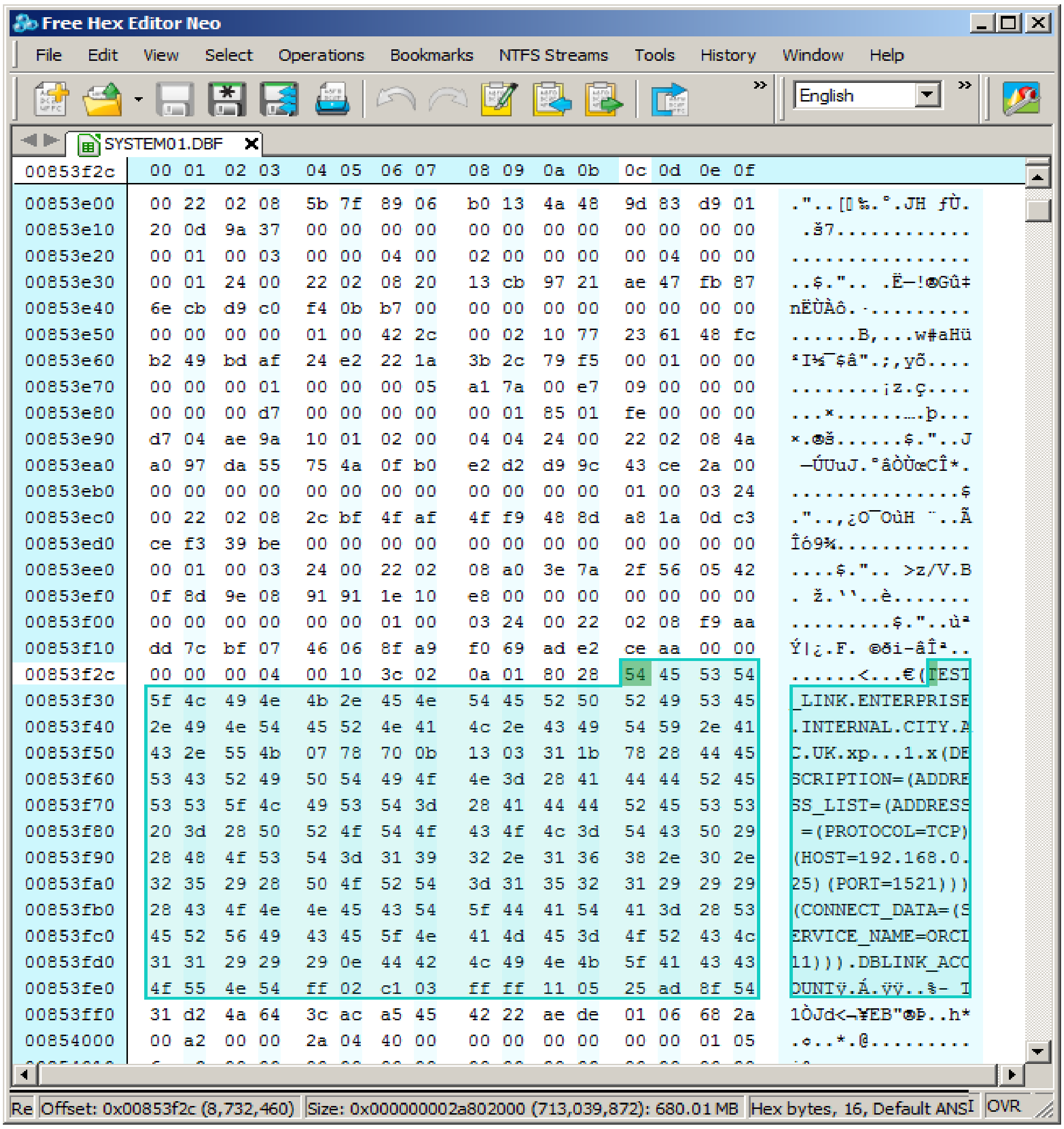
5. Forensically respond to an incident involving use of DBLink

```
SQL> select user from dual@test_link;
USER
------------------------------
SYS

SQL> drop database link test_link;

Database link dropped.
```

A dropped db link is still recorded in the `system01.dbf` as long as the data file has not filled up and re-recorded back over itself. So this evidence can be used to corroborate the `DBLINK_INFO` audit trail entry previously, to prove that the attacker's connection came from that link.



```
00853f2c   00 01  02 03   04 05  06 07   08 09  0a 0b   0c 0d  0e 0f

00853e00   00 22  02 08   5b 7f  89 06   b0 13  4a 48   9d 83  d9 01   ."..[.‰.°.JH ƒÙ.
00853e10   20 0d  9a 37   00 00  00 00   00 00  00 00   00 00  00 00    .š7............
00853e20   00 01  00 03   00 00  04 00   02 00  00 00   00 04  00 00   ................
00853e30   00 01  24 00   22 02  08 20   13 cb  97 21   ae 47  fb 87   ..$.".. .Ë—!®Gû‡
00853e40   6e cb  d9 c0   f4 0b  b7 00   00 00  00 00   00 00  00 00   nËÙÀô.·.........
00853e50   00 00  00 00   01 00  42 2c   00 02  10 77   23 61  48 fc   ......B,...w#aHü
00853e60   b2 49  bd af   24 e2  22 1a   3b 2c  79 f5   00 01  00 00   ²I½¯$â".;,yõ....
00853e70   00 00  00 01   00 00  00 05   a1 7a  00 e7   09 00  00 00   ........¡z.ç....
00853e80   00 00  00 d7   00 00  00 00   00 01  85 01   fe 00  00 00   ...×.......…þ...
00853e90   d7 04  ae 9a   10 01  02 00   04 04  24 00   22 02  08 4a   ×.®š......$."..J
00853ea0   a0 97  da 55   75 4a  0f b0   e2 d2  d9 9c   43 ce  2a 00    —ÚUuJ.°âÒÙœCÎ*.
00853eb0   00 00  00 00   00 00  00 00   00 00  00 00   01 00  03 24   ...............$
00853ec0   00 22  02 08   2c bf  4f af   4f f9  48 8d   a8 1a  0d c3   ."..,¿O¯OùH ¨..Ã
00853ed0   ce f3  39 be   00 00  00 00   00 00  00 00   00 00  00 00   Îó9¾............
00853ee0   00 01  00 03   24 00  22 02   08 a0  3e 7a   2f 56  05 42   ....$.".. >z/V.B
00853ef0   0f 8d  9e 08   91 91  1e 10   e8 00  00 00   00 00  00 00   . ž.''..è.......
00853f00   00 00  00 00   00 00  01 00   03 24  00 22   02 08  f9 aa   .........$."..ùª
00853f10   dd 7c  bf 07   46 06  8f a9   f0 69  ad e2   ce aa  00 00   Ý|¿.F. ©ði-âÎª..
00853f2c   00 00  00 04   00 10  3c 02   0a 01  80 28   54 45  53 54   ......<...€(TEST
00853f30   5f 4c  49 4e   4b 2e  45 4e   54 45  52 50   52 49  53 45   _LINK.ENTERPRISE
00853f40   2e 49  4e 54   45 52  4e 41   4c 2e  43 49   54 59  2e 41   .INTERNAL.CITY.A
00853f50   43 2e  55 4b   07 78  70 0b   13 03  31 1b   78 28  44 45   C.UK.xp...1.x(DE
00853f60   53 43  52 49   50 54  49 4f   4e 3d  28 41   44 44  52 45   SCRIPTION=(ADDRE
00853f70   53 53  5f 4c   49 53  54 3d   28 41  44 44   52 45  53 53   SS_LIST=(ADDRESS
00853f80   20 3d  28 50   52 4f  54 4f   43 4f  4c 3d   54 43  50 29    =(PROTOCOL=TCP)
00853f90   28 48  4f 53   54 3d  31 39   32 2e  31 36   38 2e  30 2e   (HOST=192.168.0.
00853fa0   32 35  29 28   50 4f  52 54   3d 31  35 32   31 29  29 29   25)(PORT=1521)))
00853fb0   28 43  4f 4e   4e 45  43 54   5f 44  41 54   41 3d  28 53   (CONNECT_DATA=(S
00853fc0   45 52  56 49   43 45  5f 4e   41 4d  45 3d   4f 52  43 4c   ERVICE_NAME=ORCL
00853fd0   31 31  29 29   29 0e  44 42   4c 49  4e 4b   5f 41  43 43   11))).DBLINK_ACC
00853fe0   4f 55  4e 54   ff 02  c1 03   ff ff  11 05   25 ad  8f 54   OUNTÿ.Á.ÿÿ..%- T
00853ff0   31 d2  4a 64   3c ac  a5 45   42 22  ae de   01 06  68 2a   1ÒJd<¬¥EB"®Þ..h*
00854000   00 a2  00 00   2a 04  40 00   00 00  00 00   00 00  01 05   .¢..*.@.........
```

Re | Offset: 0x00853f2c (8,732,460) | Size: 0x000000002a802000 (713,039,872): 680.01 MB | Hex bytes, 16, Default ANSI | OVR

More to come on new unpublished Oracle Security matters at my session on 2.30, Monday 3rd December, at UKOUG 2012 , entitled *"Intelligently Securing a Large, Globally Distributed, Database Estate" (and new book* Securing Oracle *in 2013).* *paulmwright@oraclesecurity.com*