UKOUG DBMS SIG, November 7th 2007

Oracle 11g Security

By

Pete Finnigan

Written Friday, 21st September 2007

Introduction - commercial slide.☹

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases
- http://www.petefinnigan.com
- Consultancy and training available
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA)

Agenda

- Summarise the new 11g Security features
- Identify some of the base security issues
- 11g features added to fix these issues
- Some security problems are worse in 11g?
- The new 11g password algorithm
- Review some of the new features in more detail
- Arrive at some conclusions

Summary of new features (1)

- Advanced Security Option
  - Kerberos cross realm support
  - SYSDBA strong authentication now supported
  - Full tablespace encryption available (TDE)
  - Hardware based master key protection (HSM)
- Secure out of the box
  - Audit is enabled by default
  - Built in Password complexity function
  - Built in profile

The changes are not massive and I have not tested all of them yet!

Summary of new features (2)

- Secure out of the box (cont’d)
  - Fine grained access control on PL/SQL network access
  - Improved network administration, registration and operation
    - Secure listener service registration
    - Listener secured by default to prevent unauthorised local and remote operations

Summary of new features (3)

- – Improved database communication parameters
  - Report bad packets received from protocol errors
  - Terminate or resume bad packets
  - Maximum authentication attempts
  - Control the display of the database version banner
  - Control banners for unauthorised access and for auditing users actions
- – Non anonymous LDAP is added for network naming – users must identify themselves before lookup

Summary of new features (4)

- Secure manageability
  - Integrated database security manageability
  - Virtual private catalog for RMAN
- Stronger password algorithm
  - New industry standard algorithm
  - Case sensitivity
  - Default password check built in

Summary of new features (5)

- SYSASM privilege added for ASM
- Encryption
  - Intelligent LOB compression, de-duplication and securefiles
  - Compressed and encrypted dump file sets using Oracle data pump
- XML DB Security enhancements
  - XML translation support for Oracle database XML
  - Support for Web services

Some subtle new features

- Some of the new features are not advertised as security enhancements
- We have to take time to find them all. ☺
- Some examples:
  - The DBA_USERS view no longer exposes password hashes
  - Logging is more centralised and most logs are now XML
  - DDL can be logged to the XML alert log
  - _dbms_sql_security_level prevents cursor theft

Some of the core security problems

- First lets acknowledge that Oracle recognise and understand some of the core issues – well done to Oracle!
- Core security issues with the database:
  - Leaked password hashes
  - Weak passwords and default users
  - Too many features enabled
  - No audit enabled to detect issues
  - TNS is an easy target

New features to solve the problems

- New password features
  - Case sensitive passwords, new algorithm
  - Default password checks
- Password / User management
  - Built in complexity function and profile
  - Failed logins – throttling of connections
- Network changes
  - Detect bad packets
  - More secure listener
- Prevent hash leakage from dictionary
- From 10gR2 mkstore for slash login

Some things are worse in 11g!

- Just some examples not everything!
- Public gets bigger – (figures can vary based on install)
  - 9iR2 – 12,132
  - 10gR2 – 21,530 – 77.4% more than 9iR2
  - 11gR1 – 27,461 – 27.5% more than 10gR2
- Apex is installed by default
  - Good example of attack surface increase – BAD!
  - Unless you are writing an Apex application you don’t need it
- More default users!

The new password algorithm

- SHA-1 is used but deprecated by NIST in favour of SHA-2 variants years ago?
- New algorithm is fast (not as fast as DES but fast) - should use a slow algorithm in modern password authentication
- Case sensitive (works with old clients) – links have issues.
- Salt is used – salt is sent in TNS packet - AUTH_VFR_DATA
- Old hash is available still – causes weakness
- Clever password crackers are exploiting this fact
- Password hashes different each time created

New Password Algorithm (2)

```
memcpy(data,pwd,strlen((char*)pwd));
memcpy(data+strlen((char*)pwd),salt,10);
SHA1(data,strlen((char*)pwd)+10,md);
```

- Extract from http://www.soonerorlater.hu/index.khtml?article_id=513
- Uses < 10gR2 first (non case) then cracks case
- PL/SQL simple version http://www.petefinnigan.com/sha1.sql

Case sensitivity

```
SQL> create user a identified by aa;
User created.
SQL> create user aa identified by a;
User created.
SQL> exec print_table('select name,password,spare4 from sys.user$
   where name in (''A'',''AA'')');
NAME : A
PASSWORD : 637CFFBB696F8AF9
SPARE4 :
S:8CAE3110AE48B8AC3B10365BD7F1BBD2ECB37A0DAFD01CC11939154B7DF7
-----------------
NAME : AA
PASSWORD : 637CFFBB696F8AF9
SPARE4 :
S:437572D2C884BB4BCB3C635EE8BEDF92D495C93F3E58DB300553BA18FD59
```

Weakness – old hash is there still by default

```
SQL> show parameter sec_case_sensitive_logon
sec_case_sensitive_logon       boolean     TRUE
SQL>
```

Audit is turned on by default

```
SQL> sho parameter aud

NAME                  TYPE    VALUE
--------------------- ------- ---------------
audit_file_dest       string  /oracle/admin/ORA11G/adump
audit_sys_operations  boolean FALSE
audit_syslog_level    string
audit_trail           string  DB
SQL>
```

- Audit is turned on by default to SYS.AUD$
- Privilege (23) options enabled
- Statement (24) options enabled
- No extended audit or OS audit by default

Audit is turned on by default

```
SQL> select privilege typ, success, failure from dba_priv_audit_opts
  2  union
  3  select audit_option typ, success,failure from dba_stmt_audit_opts;

TYP                                      SUCCESS   FAILURE
---------------------------------------- --------- ---------
ALTER ANY PROCEDURE                      BY ACCESS BY ACCESS
ALTER ANY TABLE                          BY ACCESS BY ACCESS
ALTER DATABASE                           BY ACCESS BY ACCESS
ALTER PROFILE                            BY ACCESS BY ACCESS
ALTER SYSTEM                             BY ACCESS BY ACCESS
ALTER USER                               BY ACCESS BY ACCESS
AUDIT SYSTEM                             BY ACCESS BY ACCESS
CREATE ANY JOB                           BY ACCESS BY ACCESS
CREATE ANY LIBRARY                       BY ACCESS BY ACCESS
CREATE ANY PROCEDURE                     BY ACCESS BY ACCESS
CREATE ANY TABLE                         BY ACCESS BY ACCESS
CREATE EXTERNAL JOB                      BY ACCESS BY ACCESS
CREATE PUBLIC DATABASE LINK              BY ACCESS BY ACCESS
CREATE SESSION                           BY ACCESS BY ACCESS
CREATE USER                              BY ACCESS BY ACCESS
DROP ANY PROCEDURE                       BY ACCESS BY ACCESS
DROP ANY TABLE                           BY ACCESS BY ACCESS
DROP PROFILE                             BY ACCESS BY ACCESS
DROP USER                                BY ACCESS BY ACCESS
EXEMPT ACCESS POLICY                     BY ACCESS BY ACCESS
GRANT ANY OBJECT PRIVILEGE               BY ACCESS BY ACCESS
GRANT ANY PRIVILEGE                      BY ACCESS BY ACCESS
GRANT ANY ROLE                           BY ACCESS BY ACCESS
ROLE                                     BY ACCESS BY ACCESS
SYSTEM AUDIT                             BY ACCESS BY ACCESS

25 rows selected.

SQL>
```

Can be extended

- More system privileges

Few things missing

- Views (rootkits)
- Alter Session (trace)

Key object audit can be added

- critical tables (AUD$...)

Default complexity function

- A new function (verify_function_11g) in $ORACLE_HOME/rdbms/admin/utlpwdmg .sql for 11g
- The script contains an identical DEFAULT profile with the function BUT
- The new password complexity function is not enabled – WHY?
- The old function is still available – be wary to not set the old one

Password complexity new checks

- Minimum length 8 chars
- Username!=password
- Username||1..100 != password
- Username (reversed) != password
- Password != server name
- Password != server name||1..100
- Simple password check (too simple, can be improved)
- Check is password = oracle||1..100
- Password has one digit + one character (where are specials?)
- Password differs from last by at least 3 characters

Default profile

```
SQL> select profile,resource_name,limit
  2  from dba_profiles
  3  order by profile,resource_name;

PROFILE  RESOURCE_NAME                    LIMIT
-------- -------------------------------- -----------
DEFAULT  COMPOSITE_LIMIT                  UNLIMITED
DEFAULT  CONNECT_TIME                     UNLIMITED
DEFAULT  CPU_PER_CALL                     UNLIMITED
DEFAULT  CPU_PER_SESSION                  UNLIMITED
DEFAULT  FAILED_LOGIN_ATTEMPTS            10
DEFAULT  IDLE_TIME                        UNLIMITED
DEFAULT  LOGICAL_READS_PER_CALL           UNLIMITED
DEFAULT  LOGICAL_READS_PER_SESSION        UNLIMITED
DEFAULT  PASSWORD_GRACE_TIME              7
DEFAULT  PASSWORD_LIFE_TIME               180
DEFAULT  PASSWORD_LOCK_TIME               1
DEFAULT  PASSWORD_REUSE_MAX               UNLIMITED
DEFAULT  PASSWORD_REUSE_TIME              UNLIMITED
DEFAULT  PASSWORD_VERIFY_FUNCTION         NULL
DEFAULT  PRIVATE_SGA                      UNLIMITED
DEFAULT  SESSIONS_PER_USER                UNLIMITED
```

- DBSNMP and WKSYS have null failed logins via separate profiles
- All other users have DEFAULT profile
- no password reuse set?
- Life time is too long
- no pwd verify function
- It’s a good start but not enough

Fine Grained Network Access

```
SQL> create user cc identified by cc;

User created.

SQL> grant create session to cc;

Grant succeeded.

SQL> connect cc/cc@ora11g
Connected.
SQL> exec dbms_output.put_line(utl_inaddr.get_host_name);
BEGIN dbms_output.put_line(utl_inaddr.get_host_name); END;

*
ERROR at line 1:
ORA-24247: network access denied by access control list (ACL)
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```

Works with UTL_TCP, UTL_SMTP, UTL_MAIL and UTL_HTTP for connections to the network and UTL_INADDR for resolve DNS requests

Access denied by default for non privileged uers

Fine Grained Network Access (2)

```
SQL> connect system/manager@ora11g
SQL> BEGIN
  2   DBMS_NETWORK_ACL_ADMIN.CREATE_ACL (
  3    acl          => 'simple_acl.xml',
  4    description  => 'Network connection permission for
   UTL_INADDR for user CC',
  5    principal    => 'CC',
  6    is_grant     => TRUE,
  7    privilege    => 'resolve');
  8  END;
  9  /
SQL> BEGIN
  2   DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL (
  3    acl         => 'simple_acl.xml',
  4    host        => '*');
  5  END;
  6  /
SQL> connect cc/cc@ora11g
SQL> exec dbms_output.put_line(utl_inaddr.get_host_name);
vostok
```

Simple ACL and assignment to all hosts for the user CC

The package can now be used correctly

Fine Grained Network Access (3)

- Package DBMS_NETWORK_ACL_ADMIN extends XDB’s ACL model to network access
- Control is limited to UTL_TCP, UTL_SMTP, UTL_MAIL, UTL_HTTP and UTL_INADDR
- Complex to set up and manage and monitor
  - Wild cards can be used
  - New ACL overrides existing – can confuse
- ACL’s control access by default for non-privileged users
- The ACL’s control network access and not package access –could be an issue

Secure Listener by Default

```
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.1.0.6.0 -
   Production
Start Date                31-OCT-2007 09:06:14
Uptime                    0 days 4 hr. 56 min. 27 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /oracle/11g/network/admin/listener.ora
Listener Log File
   /oracle/diag/tnslsnr/vostok/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=vostok)(PORT=1521)))
Services Summary...
Service "ORA11G" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
Service "ORA11GXDB" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
Service "ORA11G_XPT" has 1 instance(s).
  Instance "ORA11G", status READY, has 1 handler(s) for this service...
```

Secure Listener by default (2)

- Dynamic registration – dynamic_registration parameter – is on by default
- Only the local user who started the listener can stop it
- Xml based listener log file – old one still there also
- Remote admin with password or Cost (Class of Secure Transports)
- Downside:
  - Extproc still enabled by default
  - Extra services, XDB, XPT enabled by default
  - Default name LISTENER and port 1521 by default

Default Password Check

```
SQL> select * from dba_users_with_defpwd;

USERNAME
------------------------------
DIP
MDSYS
WK_TEST
CTXSYS
OUTLN
EXFSYS
MDDATA
ORDPLUGINS
ORDSYS
XDB
SI_INFORMTN_SCHEMA
WMSYS

12 rows selected.
```

Uses the old 10gR2 hash

No passwords available

690 records in the table

Remember if found you would still need to resolve the case sensitive password in 11g if its not all one case

Cannot be updated within a support contract?

Can implement your own version of the same

Default Password Check (2)

```
SQL> select text from dba_views
  2  where view_name='DBA_USERS_WITH_DEFPWD';

TEXT
---------------------------------------------------------------------
SELECT DISTINCT u.name
    FROM SYS.user$ u, SYS.default_pwd$ dp
   WHERE u.type#    = 1
     AND u.password = dp.pwd_verifier
     AND u.name     = dp.user_name
     AND dp.pv_type = 0

SQL> select * from sys.default_pwd$
  2  where rownum<5;

USER_NAME       PWD_VERIFIER     PV_TYPE
--------------- ---------------- -------
AASH            9B52488370BB3D77       0
ABA1            30FD307004F350DE       0
ABM             D0F2982F121C7840       0
AD_MONITOR      54F0C83F51B03F49       0
```

Connection throttling

```
SQL> show parameter sec

NAME                                 TYPE        VALUE
------------------------------------ ----------- --------
db_securefile                        string      PERMITTED
optimizer_secure_view_merging        boolean     TRUE
sec_case_sensitive_logon             boolean     TRUE
sec_max_failed_login_attempts        integer     10
sec_protocol_error_further_action    string      CONTINUE
sec_protocol_error_trace_action      string      TRACE
sec_return_server_release_banner     boolean     FALSE
sql92_security                       boolean     FALSE
```

Sec_max_failed_login_attempts works at the server level and starts a throttling process

Connection Throttling (2)

```
SQL> @conn
ERROR:
ORA-01017: invalid username/pas
Elapsed: 00:00:00.01
ERROR:
ORA-01017: invalid username/pas
Elapsed: 00:00:00.03
ERROR:
ORA-01017: invalid username/pas
Elapsed: 00:00:01.05
ERROR:
ORA-01017: invalid username/pas
Elapsed: 00:00:03.07
ERROR:
ORA-01017: invalid username/password; logon denied
Elapsed: 00:00:07.01
ERROR:
ORA-01017: invalid username/password; logon denied
Elapsed: 00:00:11.03
ERROR:
ORA-01017: invalid username/password; logon denied
Elapsed: 00:00:16.04
```

```
timing start
connect system/rubbish@ora11g
timing show
connect system/rubbish@ora11g
timing show
connect system/rubbish@ora11g
timing show
connect system/rubbish@ora11g
timing show
```

Conclusions

- Summarised the new 11g Security features
- Identified some of the base security issues
- Looked at 11g features added to fix these issues
- Review some of the new features in more detail – new passwords for example
- Not major enhancements for security but the underlying trend to fix the core issues is the major message to be taken for security in 11g.

Any Questions?

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