Oracle 11g Security
By Pete Finnigan
Written Friday, 21st September 2007

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)

```sql
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

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

Case sensitivity

- Weakness – old hash is there still by default

Audit is turned on by default

- 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

- Can be extended More system privileges Few things missing Views (readable) 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

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.

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

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    ... BEGIN  2  DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL (  3    acl => 'simple_acl.xml',  4    host        => '*');  5  END;  6  /

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 and UTL_HTTP for connections to the network and UTL_INADDR for resolve DNS requests

Secure Listener by Default

STATUS of the LISTENER
-------------------------------
Alias             LISTENER
Version           TNSLSNR for Linux: Version 11.1.0.6.0 -
Start Date        21-OCT-2007 09:04:14
Option            3 days 8 hs. 16 min. 25 sec
Trace Level       0
Security          ON: local + Authentication
SNMP              OFF
Listener Parameter File /oracle/app/oracle/tnslsnr/oracle/svcman/listener.ora
listener log File /oracle/app/oracle/tnslsnr/oracle/svcman/listener.log
listener log summary: [DESCRIPTION:ADDRESS=PROTOCOL=tcp(ADDRESS=((Proto=udp(PORT=1521))))]
Protocol Summary:
  * Disabled "SNMP" has 1 listener(s): Instant "SNMP", status READY, has 1 listener(s) for this service... 
  * Disabled "SNMP" has 1 listener(s): Instant "SNMP", status READY, has 1 listener(s) for this service... 
  * Disabled "SNMP" has 1 listener(s): Instant "SNMP", status READY, has 1 listener(s) for this service...

Default profile

- 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
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;
  SELECT * FROM dba_users_with_defpwd;
  USEM ------------------------------
  DIP MDSYS WK_TEST CTXSYS OUTLN EXFSYS MDDATA ORDPLUGINS ORDSYS XDB SI_INFORMTN_SCHEMA WMSYS
  12 rows selected.

Default Password Check (2)

- 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
  sql92_security boolean FALSE

Connection throttling

- SQL: `@conn
  ERROR: ORA-01017: invalid username/password; logon denied
  Elapsed: 00:00:00.01
  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

Connection Throttling (2)

- 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
  sql92_security boolean FALSE

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