

ORACLE®

Database Security Enhancements With Oracle Database 11g

Daniel Wong
Director of Engineering, Database Security
Oracle Corporation

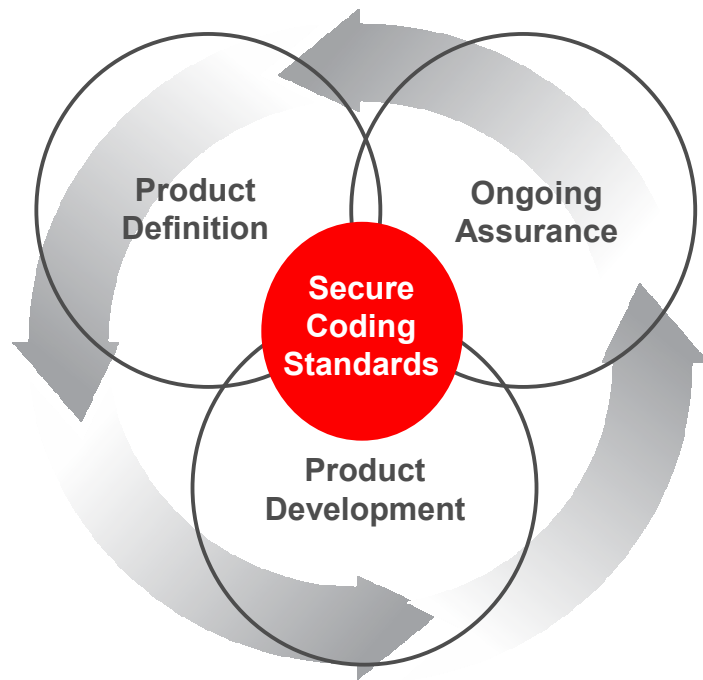
ORACLE®
DATABASE **11g**



Agenda

- About Oracle Software Security Assurance
- Overview of Security Enhancements in 11g
- Secure Configuration Enhancements
- Other Key Security Enhancements
- Q&A

Oracle Software Security Assurance



All the processes, procedures, and technologies that have been implemented to ensure that Oracle's products are meeting our customers' security requirements, while providing for the most cost-effective ownership experience.



Oracle Software Security Assurance

Secure Configuration

- Enhance “out of the box installation” settings to be more secure
 - Remove default passwords
 - Disable unneeded services
 - Reduce proliferation of powerful privileges
- Identify and minimize potential effects of enhanced secure configuration settings:
 - Impacts resulting from version upgrade
 - Impacts on Oracle and third-party applications
- Document and share current security best practices
 - <http://www.oracle.com/security/resource-library.html>



Oracle Software Security Assurance

Secure Configuration

- **Goals:**
 - Improve security of default configuration
 - Secure by Default while maintaining upgradability and usability
- **Inputs:**
 - Internal: Various Oracle Software Security Assurance programs
 - External: CIS, SANS, DISA
- **Recent Enhancements:**
 - Locked default accounts, expired passwords
 - Optional install of demo schemas
 - Best Practices document
 - Default password/account scanner



Secure Configuration Enhancements with 11g - **Overview**

1. Default Audit Settings

- Preconfigured
- Enhanced performance

2. Default Password Management

- Enhanced protection against brute force attack
- Complexity enforcement procedure
- Built-in default password scanner

3. Enhanced Authentication

- Case sensitive password authentication
- Control authentication version

4. Enhanced Access Control

- Improved security for several utl* packages



Audit Settings

- Key requirement for compliance
- 10gR2: OFF by default
- 11g:
 - AUDIT_TRAIL=DB by default in DBCA
 - security-relevant actions audited
- Performance:
 - Set audit_trail=XML or OS for best performance
 - In our informal lab environment, we found 1-2% performance degradation for the TPCC benchmark with AUDIT_TRAIL=DB and our default auditing statements



Updated Default Audit Settings

- Statement Audit option
 - ROLE
- Privilege Audit Options
 - CREATE USER
 - ALTER USER
 - DROP USER
 - CREATE SESSION
 - CREATE ANY TABLE
 - ALTER ANY TABLE
 - DROP ANY TABLE
 - CREATE ANY PROCEDURE
 - ALTER ANY PROCEDURE
 - DROP ANY PROCEDURE
 - ALTER PROFILE
 - DROP PROFILE
 - GRANT ANY PRIVILEGE
 - GRANT ANY OBJECT PRIV.
 - GRANT ANY ROLE
 - CREATE ANY JOB
 - CREATE EXTERNAL JOB
 - CREATE ANY LIBRARY
 - CREATE PUBLIC DB LINK
 - EXEMPT ACCESS POLICY
 - ALTER DATABASE
 - ALTER SYSTEM
 - AUDIT SYSTEM



Default Profile Password Settings

- 10gR2
 - FAILED_LOGIN_ATTEMPTS = 10
 - all others: unlimited
- 11g - more restrictive
 - FAILED_LOGIN_ATTEMPTS = 10 (no change)
 - PASSWORD_LOCK_TIME = 1
 - PASSWORD_GRACE_TIME = 7
 - PASSWORD_LIFE_TIME = 180
- Balanced protection against Denial of Service (DOS) and password attacks while keeping usability



Password Complexity

- Supports case sensitive passwords
 - Supports special and multi-byte characters to increase security and usability
 - Takes effect immediately after password change
- Enhanced default password complexity verification
 - Password Complexity Verification not enabled in default profile; can be enabled via Enterprise Manager or SQL
 - In utlpwdmg.sql in \$ORACLE_HOME/admin directory
 - SQL to set the password complexity verification
 - ALTER PROFILE DEFAULT PASSWORD_VERIFY_FUNCTION *verify_function_11G*
 - This routine will verify that password
 - Has minimum length of 8 characters
 - Has at least one letter and one digit
 - Is not username, reverse thereof, or username(1-100)
 - Is not one of a few common passwords (e.g. welcome1)
 - Must differ from previous password by at least 3 characters



Password Complexity Recommendations

- Default password profile parameters may not suit everyone
- Adjust the password settings to your security needs
- Change default password verification routine as per your needs
- Define at least two password profiles - one for users and one for mid-tiers and administrators
- Password recommendations vary with use cases:
 - See for example, recommendations for E-Business Suite - MetaLink 189367.1
- See also Visit OTN: otn.oracle.com -> products -> database -> security and compliance for detailed recommendations



Default Password View

- View `DBA_USERS_WITH_DEFPWD` will show all accounts still using default passwords
- Over 140 default username/passwords collected from the field, including application accounts for Peoplesoft and Ebizs

- `SQL> desc DBA_USERS_WITH_DEFPWD`
- `Name Null? Type`
- -----
- `USERNAME NOT NULL VARCHAR2(30)`

- `SQL> select * from DBA_USERS_WITH_DEFPWD`
- `2 ;`

- `USERNAME`
- -----
- `JONES`



Enhanced Authentication

- Supports multi-bytes and special characters
- Case sensitive passwords always enforced
 - Use `SEC_CASE_SENSITIVE_LOGON` to turn it OFF if necessary
- Set `SQLNET.ALLOWED_LOGON_VERSION` to highest OCI client version in use:
 - Use 8 if there are Oracle 8.x clients connecting to the DB
 - Use 9 if there are Oracle 9.x clients connecting to the DB
 - Use 11 if there are Oracle 10.x and/or 11.x clients connecting to the DB
 - Use 8 if there are pre-Oracle 11g JDBC pure Java client connecting to the DB
- Use of SHA-1 hashing algorithm to protect password



Enhanced Access Control

- Improved security for several utl* packages
 - UTL_TCP, UTL_SMTP, UTL_MAIL, UTL_HTTP, etc.
 - These packages will no longer allow connections to external network services to non-privileged users by default
- SYS and XDB schemas will specifically remain excluded from this kind of restriction
- DBAs will be able to specify what network services database users will be allowed to access when using these packages.



Enhanced Access Control

Recommendations

- Open access to external network services only minimally
 - Specify down to hosts and ports, avoid unnecessary “*” wildcards
- Have small number of ACLs for manageability and performance
 - Share ACLs among network services open to the same users
- Consider giving access indirectly through application schemas
 - Applications can further restrict user interaction with network services



Access Control Administration

- Administration via `DBMS_NETWORK_ACL_ADMIN`
 - Grant access to a network service
 - `create_acl` – create an ACL for the first user
 - `assign_acl` – assign ACL to network service
 - Grant access to more users in ACL – `add_privilege`
 - Revoke access from users in ACL – `delete_privilege`
 - Stop access to network services
 - `unassign_acl` – take ACL away from network service
 - All ACL changes are transactional
 - Remember to “COMMIT” the transaction !!!
- View ACL settings via dictionary views
 - `DBA_NETWORK_ACLS` – which network services have ACLs?
 - `DBA_NETWORK_ACL_PRIVILEGES` – who are in the ACLs?



Access Control Administration Example

```
begin
  dbms_network_acl_admin.create_acl(
    acl          => 'smtp-access.xml',
    description => 'ACL for SMTP service',
    principal    => 'MAILAGENT',
    is_grant     => TRUE,
    privilege    => 'connect');

  dbms_network_acl_admin.assign_acl(
    acl          => 'smtp-access.xml',
    host         => 'smtp-host.oracle.com',
    lower_port   => 25);
end;
/
commit;
```



Access Control Administration Example

```
SQL> select * from dba_network_acls;
```

HOST	LOWER_PORT	UPPER_PORT	ACL
smtp-host.oracle.com	25	25	/sys/acls/smtp-access.xml

```
SQL> select * from dba_network_acl_privileges;
```

ACL	PRINCIPAL	PRIVILEGE
/sys/acls/smtp-access.xml	MAILAGENT	connect



How Do These Changes Impact Installation?

- Default new installations will include audit and password profiles
- Option during install to retain 10gR2 settings
- DBCA screens to:
 - Revert back to 10gR2 settings for audit and/or password
 - Apply new default settings
- Upgrades will not change the audit and password profile settings



Recommendations for Upgrades I

- Audit settings
 - Turn on auditing for security sensitive DDL operations listed
 - Set to DB or DB_extended for querability
 - Set to OS or XML for performance
- Password Management
 - Institute password policies by classifying users into a different usage groups and assign dedicated profiles to each group
 - Check DBA_USERS_WITH_DEFPWD for default passwords



Recommendations for Upgrades II

- Authentication
 - Identify sources of connection and set security level to highest possible supported by the client
 - Ask users to change password as soon as possible for case sensitive password to take effect
 - Look into EUS for centralized user management
 - Reminder: we support connect username/password as SYSDBA
- Access Control
 - Identify applications using utl_* packages, and identify and grant appropriate new ACL privileges and confirm applications are running fine
 - Evaluate current privileges granted, follow least privileged model



Other Key Security Enhancements

- Tablespace Encryption option in Transparent Data Encryption
 - Allows bulk encryption at tablespace level
 - No restriction on data types and indexes
 - Works with all High Availability offerings
- Hardware Security Module and External Key Server support in Transparent Data Encryption
 - Provides additional option for security and key management services by third party products
- Management of SYSDBA and SYSOPER in Enterprise User Security
 - Identity management of super users in databases
- Enhanced Kerberos support
 - Cross realm and type 4 certificate support
 - Support Microsoft KDC default encryption modes

Oracle Software Security Assurance

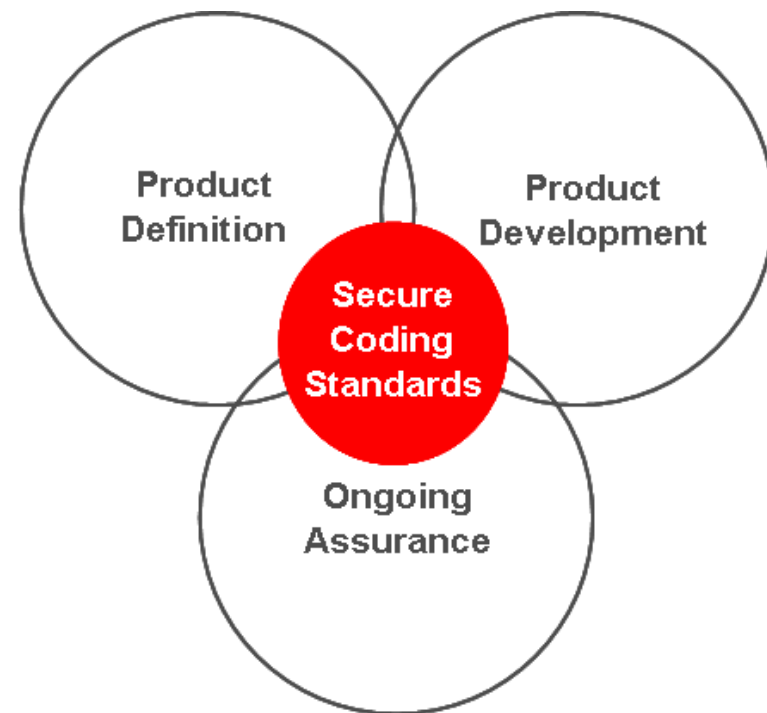
Conclusion

- **MAXIMUM SECURITY**

- Best of breed security features
- Secure design from the ground up
- Effective vulnerability remediation process

- **LOWER COST OF OWNERSHIP**

- Unwavering commitment to maintaining our customer's security posture
- Predictable security patch process
- Priority given to quality





For More Information

- **Oracle Software Security Assurance Web Site** at <http://www.oracle.com/security/software-security-assurance.html>
 - Technical white papers and security guides
 - Online security seminars and webcasts
 - Blogs and more
- **Critical Patch Update & Security Alerts** at <http://www.oracle.com/technology/deploy/security/alerts.htm>
 - Critical Patch Updates and current security alerts
 - Patch download
 - CPU documentation & Risk Matrices

<http://search.oracle.com>

Oracle Software Security Assurance

