JIBE

Management & Technology Consulting

How to Protect your Oracle Database From Hackers

Presented By:
Jeff Kayser

JIBE

Who is Jeff Kayser

- Oracle E-Business Suite DBA Since 1989 (RDBMS 5, E-Business Suite MPL 6)
- Supported many Portland Oracle Shops.
  - Sequent Computers
  - Nike
  - OHSU
- Interested in Oracle Security for a long time.
- Works for Jibe Consulting.

Who is Jeff Kayser Cont.

- Credited in 3 CPU security notes:
  - Oracle Critical Patch Update – October 2006
  - Oracle Critical Patch Update Advisory – October 2008
  - Oracle Critical Patch Update Advisory – July 2013
  - A forth security issue, for Oracle's Hyperion software product, is currently being worked by Oracle Development.

Potential Logging of E-Business Suite Passwords

- Late last year, I detected a password disclosure issue with E-Business Suite R12, and reported it to Oracle. After I made sure that Oracle Support could replicate the issue, Oracle E-Business Suite Development worked the issue. The password disclosure issue has now been addressed in the July 2013 CPU security patch.

Potential Logging of E-Business Suite Passwords

- The Carnegie Mellon CERT organization has issues a public advisory about this issue. You can see the advisory here:
- http://www.kb.cert.org/vuls/id/826463
- As noted in the Oracle Security Alert, the CVE number is: CVE-2013-3749
- **MOS note: Potential Logging of E-Business Suite Passwords (Doc ID 1579709.1)**

Potential Logging of E-Business Suite Passwords

View this message in a Web browser

ORACLE

Dear Oracle Customer,

You are receiving this e-mail because you are an E-Business Suite Customer.

A fix to address vulnerability CVE-2013-3749, which resulted in EBS passwords being inadvertently logged to diagnostic logs, has been released in the July 2013 CPU. This accidental password logging may occur in diagnostic tables and/or log files depending on how logging is configured. While these log files are generally only accessible to administrators, it is important to ensure that any E-Business Suite instances affected by this vulnerability be fixed, and that any impacted log files are purged or have the inadvertent entries removed.

This vulnerability will affect all customers who use E-Business Suite native login pages (local login), and have applied any of the E-Business Suite Critical Patch Update patches between July 2012 to April 2013 or the one-off patches 10009066 or 12832734. SSO/OAM customers will be impacted if they use the local login page for some logins.

Please see My Oracle Support (MOS) Note 1579709.1 for more information on the mitigation steps for this issue, and how to remove these entries in your log files.

Potential Logging of E-Business Suite Passwords

- You are affected if you have applied any of the E-Business Suite CPU patches: July 2012, Oct 2012, Jan 2013, or Apr 2013. There are also two one-off patches identified that cause the same issue: 12832734 and 10009066. See the MOS note for the latest news about which patches introduce the problem.

- If you are affected, please follow the mitigation steps in the note to ensure that your E-Business Suite system is secured.

Potential Logging of E-Business Suite Passwords

- **Note: Even if you have already applied CPU July 2013, you still need to read the note, because some of the mitigation steps will still apply.**

- I recommend doing the optional password change mitigation step (as well as the other mitigation steps).

Why Database Security?

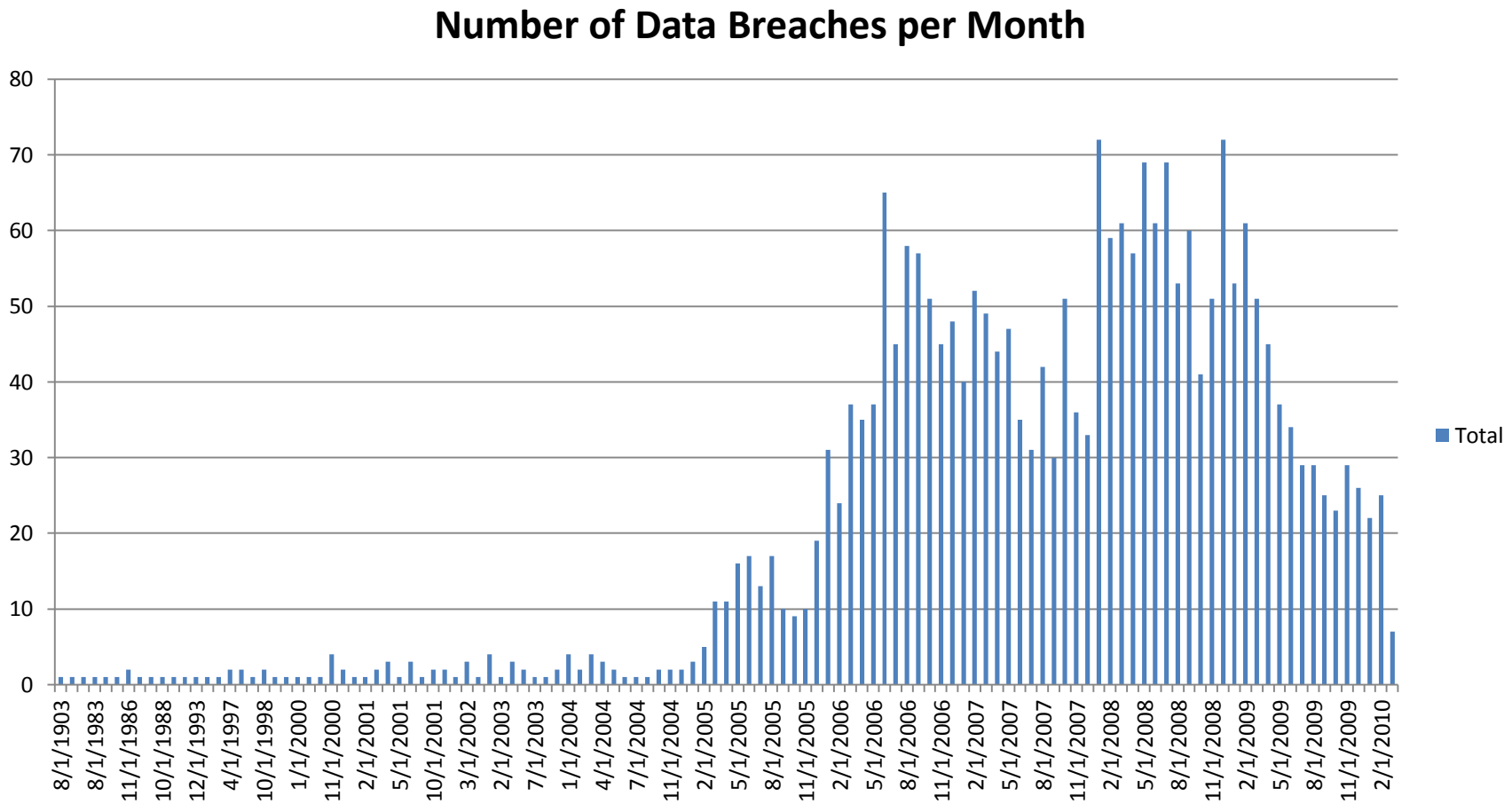
There are two major reasons why Companies should be interest in Database Security – **Data Breaches** and **Compliance**

- **Data Breaches**: Information about your patients can be useful to identity thieves. There are a number of websites that track data breaches. Data breaches are common, averaging more than one data breach per day. The cost of recovering from a data breach is significant. For the Healthcare industry, one current report states that the average cost is $282 per breached record.

- **Compliance**: There are many compliance requirements. External requirements include HIPAA, Sarbanes Oxley, PCI DSS, various data privacy laws, state data breach laws, industry regulations, etc. Internal requirements include security policies and standards set by the corporate Information Security group.

In order to achieve a return on your investment in Database Security, a company must have a Strategy and follow a road map

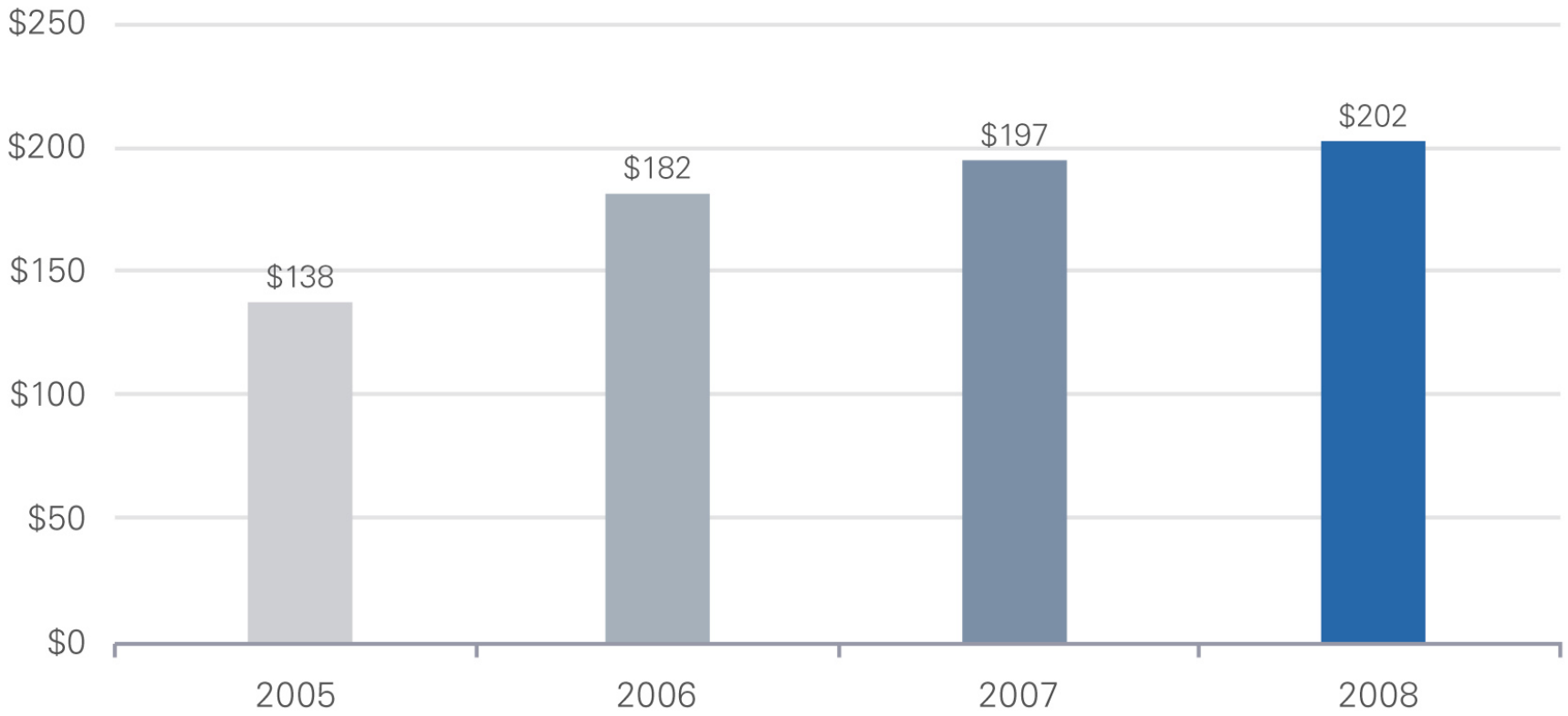
Why Database Security?



Publicly-Known Data Breaches (http://datalossdb.org)

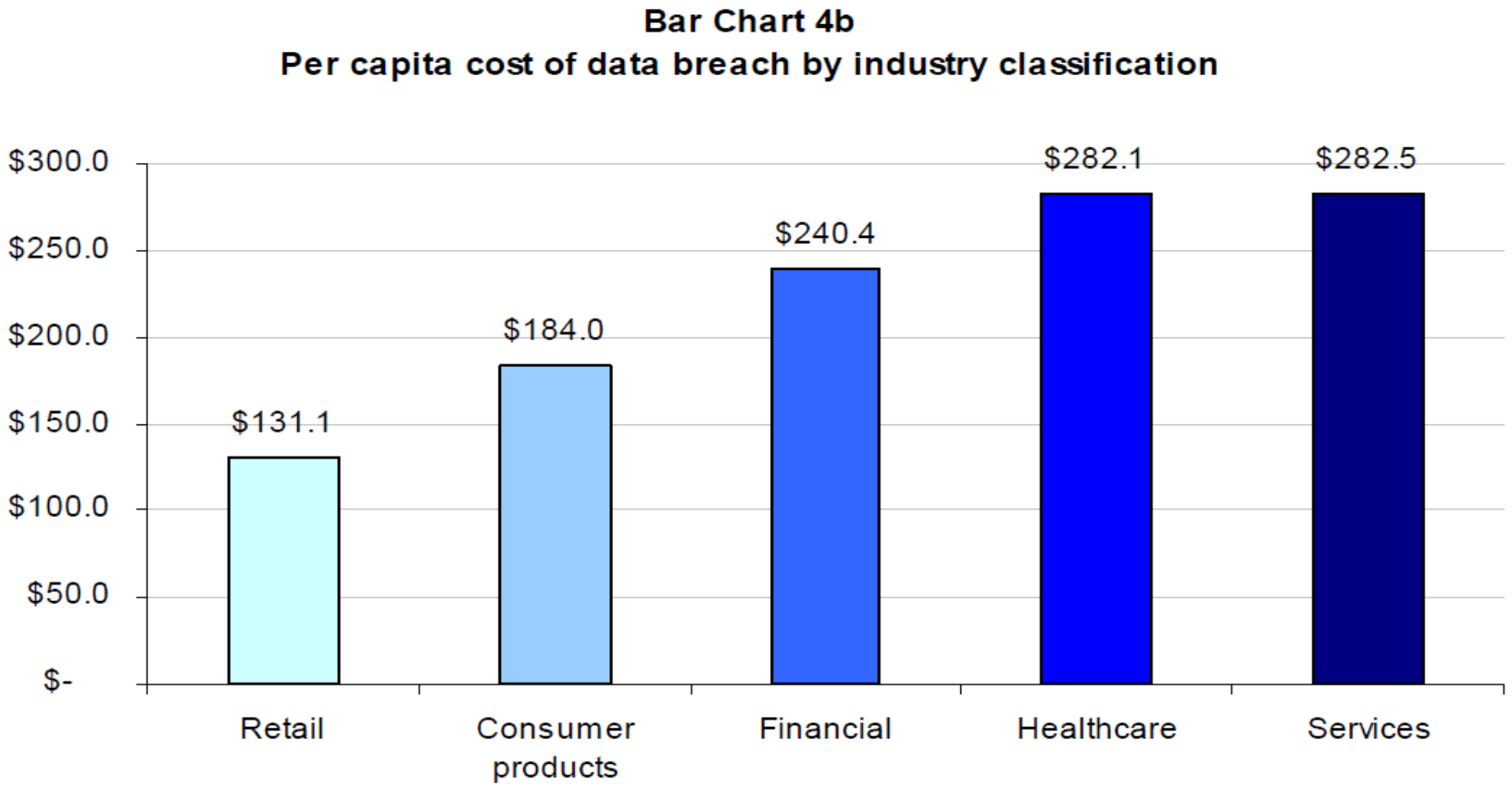
Why Database Security?

Average Cost of a Data Breach (per record lost)



Source: 2008 Annual Study: Cost of a Data Breach
(Performed by Ponemon Institute, Sponsored by PGP Corporation)

Why Database Security?



Source: 2009 Annual Study: Cost of a Data Breach
(Performed by Ponemon Institute, Sponsored by PGP Corporation)

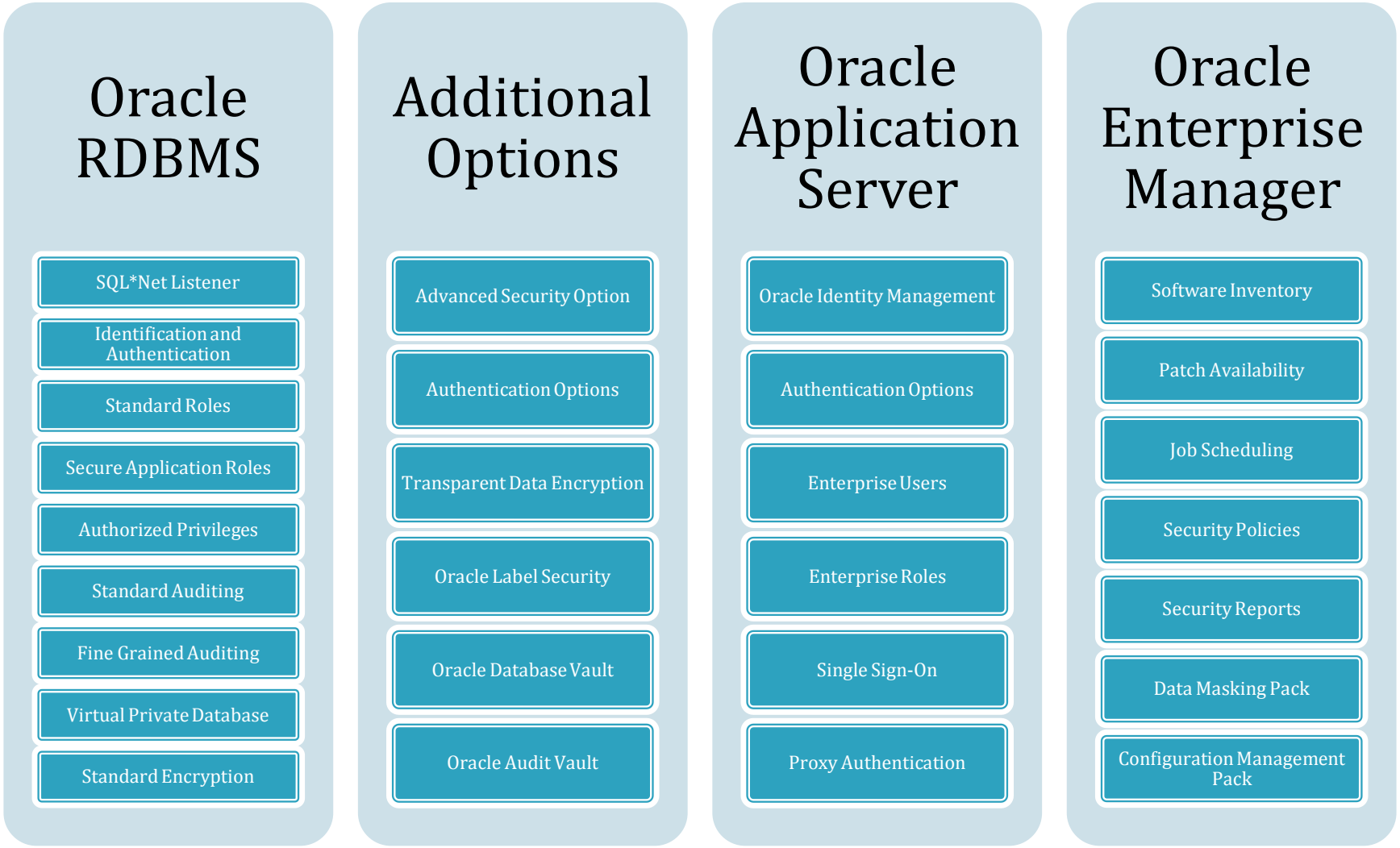
Why Database Security?

- External Compliance Requirements:
  - HIPAA.
  - Sarbanes Oxley.
  - Payment Card Industry Data Security Standard.
  - ARRA: American Recovery and Reinvestment Act of 2009. Data breach of unsecured PHI requires notification starting 9/15/09.
  - Other Data Privacy and Data Breach Laws.

A note about HIPAA & DB Security

- **Security standards: General rules:**
  - Ensure the confidentiality, integrity, and availability of all EPHI.
  - Protect against anticipated threats or hazards to the security or integrity of EPHI.
  - Protect against anticipated unauthorized uses or disclosures of EPHI.
- **Technical safeguards:**
  - *Access control:* Required: *Unique user identification, Emergency access procedure.* Addressable: *Automatic logoff, Encryption and decryption.*
  - *Audit controls:* Required: for activity that uses EPHI.
  - *Integrity:* Addressable: *Mechanism to authenticate electronic protected health information.*
  - *Person or entity authentication:* Required: to authenticate users of EPHI.
  - *Transmission security:* Addressable: *Integrity controls, Encryption.*
- **EPHI:** *Electronic protected health information.* Individually identifiable health information is protected. For example: names, dates, addresses or locations, telephone#, fax#, email, SSN, Med Rec#, License plate, etc.)

Oracle's Security Product Map



Jibe At-A-Glance

ORACLE Platinum Partner

Established: 2004

Employees: 130+

Customers: 200+ Over 1000 Projects

Industry Focus: Retail, Manufacturing (process, industrial & high tech), Consumer Products, Oil & Gas, Engineering and Construction, Life Sciences, Healthcare, Software and Clean Technologies

Principal business areas:

Management Consulting

- Business & IT Alignment Strategy
- Business & Technology Strategy
- Lean Enterprise Process Analysis & Design
- Program / Project Management

Technology Consulting

- ERP Implementations
- Edge Products – PLM, CRM, EPM
- Information Management & Business Intelligence
- Managed Services & Hosting

Technology Practice

The Resources

- Oracle Gold Partner – Certified Since 2004
- Certified Microsoft Partner Since 2006
- IBM Business Partner
- Authorized reseller of Oracle Products and Education
- Dedicated Technology consultants local to the PNW & RMR
- 12+ years average industry experience; 8+ years average technology experience
- 100% of consultants certified in relevant software or industry accreditations
- Managed Services Organization
  - Onshore resources
  - Remote systems management
  - Hosting
  - Virtualization
  - Project Jumpstarts

The Experience

- Business Intelligence
- Enterprise Performance Management
- Data Warehousing
- Database installation & Upgrades
  - RAC / Grid
  - High Availability
- Security Assessments
- Managed Services
  - Security
  - DBMS
  - Hosting
- Virtualization of Database & Packaged Software (ERP, EPM, BI)
- SOA Enablement
  - ESB, Canonical Modeling
- Agile based project development methodology for Iterative prototyping and rapid implementation techniques

The Tools

- Comprehensive Security Audits with Oracle best practices & 3rd party security tools
- Complete systems management & monitoring with Oracle Enterprise Manager
- Extensive Business Intelligence Solutions with Hyperion, OBIEE, Informatica, Discoverer & Oracle Data Integrator
- Experts in Oracle Virtualization, including VMWare, virtual clustering & Storage infrastructure

Jibe's Security Approach

- **Review**: Set scope and review environment.
- **Inform**: Inform client about security metrics.
- **Assess**: Measure security using chosen metrics.
- **Rank**: Rank issues based on risk.
- **Recommend**: What needs to be done to improve database security?

Oracle's Security Checklist

- Jibe Consulting commends Oracle Corporation on providing an excellent checklist for establishing a security baseline for Oracle databases.
- Jibe Consulting has enhanced this to provide metrics (for measuring compliance to this security baseline), and processes (for determining compliance).
- Where appropriate, Jibe Consulting has also added commentary about security issues related to items in the security checklist.

INSTALL ONLY WHAT IS REQUIRED

- “The Oracle Database software installation has two modes - typical and custom. For production systems, the custom installation mode can be used to install the minimum set of features and options required. If in the future, you wish to install additional features or options, simply re-run the Oracle installer.

INSTALL ONLY WHAT IS REQUIRED

- When installing RDBMS, use “custom” to install minimal set of features.

- Do not install sample schemas

INSTALL ONLY WHAT IS REQUIRED

- **METRIC: Only the minimum Oracle software needed to do the job is installed.**
- **METRIC: XDB listener is not activated if it is not needed.**
- **METRIC: XPT listener is not activated if it is not needed.**
- **METRIC: Sample schemas are not installed.**
- **METRIC: If Sample schemas are installed, the accounts are locked.**

INSTALL ONLY WHAT IS REQUIRED

- 416132.1: XML Database FAQ
- 362540.1: How to Setup XDB Protocol Server: FTP, HTTP, WebDAV
- Disable the XDB-specific dispatchers, and restart the listener.
- 742156.1: 9iR2: How to Determine if XDB is Being Used in the Database?
- 742113.1: 10g: How to Determine if XDB is Being Used in the Database?
- 733667.1: 11g: How to Determine if XDB is Being Used in the Database?
- 274508.1: Listener Issue: Removing XDB Handlers for HTTP and FTP Ports 8080 and 2100

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

- “The Oracle database installs with a number of default (preset) user accounts. Each account has a default (preset) database password. After successful installation of the database the database configuration assistant (DBCA) automatically locks and expires most default database user accounts. In addition, the password for accounts such as SYSTEM are changed to the value specified during database installation.

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

- **METRIC: Most default accounts are locked and expired.**

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

- The following SQL can be used to lock and expire database accounts.

sqlplus> connect mydba

sqlplus> alter user jsmith account lock and expire”

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

```
select username, account_status
from dba_users
where username in (
'ADAMS', 'ANONYMOUS', 'APEX_PUBLIC_USER',
'AURORA$ORB$UNAUTHENTICATED',
'BI', 'BLAKE', 'CLARK', 'CTXSYS', 'DBSNMP', 'DIP', 'DMSYS', 'EXFSYS',
'FLOWS_03000', 'FLOWS_FILES', 'HR', 'IX', 'JONES', 'LBACSYS', 'MDDATA',
'MDSYS', 'MGMT_VIEW', 'ODM', 'ODM_MTR', 'OE', 'OLAPSYS', 'ORACLE_OCM',
'ORDPLUGINS', 'ORDSYS', 'OUTLN', 'OWBSYS', 'PERFSTAT', 'PM', 'QS',
'QS_ADM', 'QS_CB', 'QS_CBADM', 'QS_CS', 'QS_ES', 'QS_OS', 'QS_WS',
'RMAN', 'SCOTT', 'SH', 'SI_INFORMTN_SCHEMA', 'SPATIAL_CSW_ADMIN_USR',
'SPATIAL_WFS_ADMIN_USR', 'SYS', 'SYSMAN', 'SYSTEM', 'TRACESVR', 'TSMSYS',
'WKPROXY', 'WKSYS', 'WK_TEST', 'WMSYS', 'XDB', 'XS$NULL'
)
order by username;
```

LOCK AND EXPIRE DEFAULT USER ACCOUNTS

The most foolproof way?

- Develop and test a password change procedure for all places where passwords are used:
  - VPN
  - OS
  - Database
  - Middle-tier
  - Applications (E-Business Suite, etc.)
- Generate random, long, complex passwords.
- Change ALL passwords.

CHANGE DEFAULT USER PASSWORDS

- “Choosing secure passwords and implementing good password policies are by far the most important defense for protecting against password based security threats. Oracle recommends customers use passwords at least 10 values in length. In addition, the complexity of the password is critical. Passwords that are based on dictionary words are vulnerable to "Dictionary based attacks".

CHANGE DEFAULT USER PASSWORDS

- A complex password should contain:
  - At least 10 values in length
  - A mixture of letters and numbers
  - Contain mixed case (Supported in Oracle Database 11g)
  - Include symbols (Supported in Oracle Database 11g)
  - Little or no relation to an actual word

CHANGE DEFAULT USER PASSWORDS

- **METRIC: Password must be at least 10 characters in length.**
- **METRIC: Password must have both letters and numbers.**
- **METRIC: Password must have symbols ("_$#" are allowed prior to 11g).**
- **METRIC: Password must have little or no relation to an actual word.**

CHANGE DEFAULT USER PASSWORDS

- Prior to 11g: There are some Oracle password cracking programs that, given the password hash, can determine the password. If the password is short and simple, the cracking programs can obtain the password fairly quickly. If the password is long and complex, it takes much longer for the cracking programs to determine the password.

CHANGE DEFAULT USER PASSWORDS

- Given this:
  1) Choose long, complex passwords.
  2) Change passwords reasonably often.
  3) Protect the password hashes.

Password hashes are found in SYS tables and also in the password file in ?/dbs/orapw* files.

CHANGE DEFAULT USER PASSWORDS

The most foolproof way?

- Develop and test a password change procedure for all places where passwords are used:
  - VPN
  - OS
  - Database
  - Middle-tier
  - Applications (E-Business Suite, etc.)
- Generate random, long, complex passwords.
- Change ALL passwords.

CHANGE PASSWORD FOR ADMINISTRATIVE ACCOUNTS

- "While you can use the same password for administrative accounts such as SYSTEM, SYSMAN and DBSNMP, Oracle recommends using different passwords for each. In any Oracle environment, be it production or test, assign strong and distinct passwords to these administrative accounts."

- **METRIC: Passwords on Administrative accounts are distinct.**

- **METRIC: Passwords on Administrative accounts are strong.**

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- "The default account SCOTT no longer installs with the default password TIGER. The account is now locked and expired upon install. All other accounts installed with a default password that is the same as the user account. If any of these accounts is unlocked, assign a new stronger password. Starting with Oracle Database 11g security administrators can easily check for default passwords by using the new database view DBA_USERS_WITH_DEF_PWD."

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- **METRIC: All open accounts have non-default passwords.**

- HOW TO CHECK: Run default password scanners.
  - Oracle's default password scanner:
  - MOS note 361482.1: Frequently Asked Questions about Oracle Default Password Scanner.
  - Patch 4926128: ORACLE DEFAULT PASSWORD SCANNER

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- 3rd-party default password scanners:
- Pete Finnigan's password scanner:
  - http://www.petefinnigan.com/default/default_password_checker.htm
- NGS Squirrel for Oracle
  - http://www.ngssoftware.com/products/database-security/ngs-squirrel-oracle.php

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- Default password scanners are not all alike. For example, if you compare the Oracle default password scanner (from patch 4926128) and Pete Finnigan's default password scanner, you will find many different username, hash_value combinations that are checked. So, it is good to run multiple default password scanners.

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- A better solution would be to evaluate all accounts. If an account is not a person account, you should ensure that the password is not defaulted. One way to do this is to change the passwords to strong passwords. The Oracle Database Security Checklist has some guidelines for strong passwords.

CHANGE DEFAULT PASSWORDS FOR ALL USERS

- One possible method is to use long, randomly-generated passwords. (You can store them in a password safe – randomly generated passwords are difficult to memorize). If you want to use that method, some random password generators can be found here:

- https://secure.pctools.com/guides/password/
- http://keepass.info/

CHANGE DEFAULT PASSWORDS FOR ALL USERS

The most foolproof way?

- Develop and test a password change procedure for all places where passwords are used:
  - VPN
  - OS
  - Database
  - Middle-tier
  - Applications (E-Business Suite, etc.)
- Generate random, long, complex passwords.
- Change ALL passwords.

ENFORCE PASSWORD MANAGEMENT

- “Oracle recommends customers enforce failed login, password expiration, password complexity and reuse policies using Oracle profiles and follow best practices defined by Oracle Applications. Oracle Database 11g provides an optional installation choice that will pre-configure a default profile to enforce password expiration and reuse. Oracle recommends that basic password management rules be applied to all user passwords and that all users be required to change their passwords periodically.”

ENFORCE PASSWORD MANAGEMENT

- **METRIC: Accounts are locked out after a certain number of failed logins.**
- **METRIC: Password expiration is implemented.**
- **METRIC: Password reuse policies are implemented**

ENFORCE PASSWORD MANAGEMENT

- HOW TO CHECK: Examine the password-related settings in the profiles.

```
select * from dba_profiles
where resource_name like '%PASSWORD%';
```

ENFORCE PASSWORD MANAGEMENT

- Sample Profile settings:

- ALTER PROFILE xys LIMIT PASSWORD_REUSE_TIME 30 PASSWORD_REUSE_MAX 5;
- The last 5 passwords cannot be reused. Users must wait 30 days before changing their passwords again.

- ALTER PROFILE xyz LIMIT PASSWORD_LIFE_TIME 83 PASSWORD_GRACE_TIME 7;
- Password expires after 90 days. Warnings are issues 7 days before password expiration.

ENFORCE PASSWORD MANAGEMENT

- ALTER PROFILE xyz LIMIT FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME UNLIMITED;

- After 3 failed login attempts, the account is locked. You have to manually unlock the account before it can be used again.

ENFORCE PASSWORD MANAGEMENT

- Number of accounts with passwords that have never been changed:

```
select count(*) from sys.user$
where user# in (select user_id from dba_users
where account_status = 'OPEN')
and (
(ptime is null)
or
(ptime is not null
and ptime <= ctime)
);
```

ENFORCE PASSWORD MANAGEMENT

- Oldest password change time:

```
select min(ptime) from sys.user$
where user# in (select user_id from dba_users
where account_status = 'OPEN')
and ptime is not null
and ptime > ctime;
```

SECURE BATCH JOBS

- Secure External Password Store

"The Secure External Password Store feature introduced with Oracle Database 10g Release 2 is designed to help secure batch jobs that authenticate to the database using username / password credentials. The secure external password store uses an Oracle Wallet to hold one or more user name/password combinations to run batch processes and other tasks that run without user interaction.

SECURE BATCH JOBS

- **METRIC: Secure Password Store is used to authenticate batch jobs**

SECURE BATCH JOBS

- HOW TO CHECK:
- How do batch jobs connect to the database? If they need database passwords supplied, then the password needs to be cached somewhere and supplied to the batch job so it can connect to the database.

- In 10gR2, there is a feature called the Secure Password Store. This allows you to use an Oracle Wallet to store login credentials for one account per TNS alias. This means that plaintext passwords are not stored anywhere on the system.

SECURE BATCH JOBS

- Resources:
  - Oracle® Database Security Guide 10g Release 2 (10.2), Chapter 9 Secure External Password Store.
  - MOS note 340559.1: Using The Secure External Password Store.
  - MOS note 759226.1: How To Maintain Multiple Wallets For A Single Database Instance.

SECURE BATCH JOBS

- Notes:
  - The sqlnet.ora file location: $TNS_ADMIN/sqlnet.ora, $HOME/.sqlnet.ora
  - Each Secure Password Store can contain only 1 username/password setting per TNS alias.

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- “Special attention should be given to managing access to the SYSDBA and SYSOPER roles. As with any database role, careful consideration should be given when granting these roles. Oracle recommends customers refrain from connecting with the SYSDBA role except when absolutely required such as called for by an existing Oracle feature or patching. Moving forward Oracle will be eliminating all dependencies on direct connections using SYSDBA. Large and small organizations should create separate administrative accounts.

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- **METRIC: Database administrators use SYSDBA and SYSOPER login privileges only when necessary.**
- **METRIC: Unsuccessful SYSDBA and SYSOPER connections are audited.**
- **METRIC: Audit logs are monitored for unsuccessful SYSDBA and SYSOPER connections.**

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- HOW TO CHECK:
  - Ask the DBAs if they only use SYSDBA and SYSOPER privileges when needed.

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- Make sure auditing is enabled.
- INIT.ORA: AUDIT_TRAIL:
- alter system set audit_trail=os scope=spfile;

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- Write text file to ADUMP destination.
- Writing audit trail records to the OS is recommended by Oracle.
- Other possible settings are:
- alter system set audit_trail=db scope=spfile;

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- Write to AUD$
- alter system set audit_trail='db','extended' scope=spfile;

- Write to AUD$ with SQL statements.
- 249438.1: 10G: New Value DB_EXTENDED for the AUDIT_TRAIL init.ora Parameter
- alter system set audit_trail='xml' scope=spfile;

MANAGE ACCESS TO SYSDBA AND SYSOPER ROLES

- Write XML file to ADUMP destination.

- alter system set audit_trail='xml','extended' scope=spfile;

ENABLE ORACLE DATA DICTIONARY PROTECTION

- “Oracle recommends that customers implement data dictionary protection to prevent users who have the "ANY" system privileges from using such privileges to modify or harm the Oracle data dictionary.

- To enable data dictionary protection, set the O7_DICTIONARY_ACCESSIBILITY parameter to FALSE. This can be accomplished by using Oracle Enterprise Manager Database Control

ENABLE ORACLE DATA DICTIONARY PROTECTION

- **METRIC: Data Dictionary Protection is enabled.**
- HOW TO CHECK:
- Ensure that INIT.ORA parameter O7_DICTIONARY_ACCESSIBILITY = FALSE.

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- "Oracle recommends you avoid granting powerful privileges to new database users, even privileged users. The Oracle DBA role should be granted with caution and only to those privileged user who need full DBA privileges. Special attention should be given when assigning privileges to application schemas. Access to the SYSDBA role should be granted with extreme care and only to those who are in the most trusted position. Auditing should be used to monitor all activities of users connecting with the SYSDBA role or other administrative roles such as the DBA role, CREATE ANY TABLE privilege and so forth. For optimal auditing performance set your audit destination to point to the operating system."

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- **METRIC: The DBA role is only granted to users who need full DBA privileges.**
- **METRIC: The SYSDBA privilege is only granted to users who need SYSDBA privileges.**
- **METRIC: The "… ANY …" privileges are only granted to users who need those privileges.**
- **METRIC: All activities of users connecting with the SYSDBA role are audited.**
- **METRIC: All activities of users who have the DBA role are audited.**
- **METRIC: All usage of "…ANY…" privileges is audited.**

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- HOW TO CHECK:
- To see which users have the DBA role:
- http://www.petefinnigan.com/who_has_role.sql

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- To see which users have the SYSDBA role:

```
select * from v$pwfile_users;
```

- To see which users have "…ANY…" privileges:

```
select grantee, count(*) num_any_privs from
dba_sys_privs
where privilege like '% ANY %'
group by grantee;
```

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- If you wish to delve deeper into specific privileges, you can use the script:
  - http://www.petefinnigan.com/who_has_priv.sql

- To check to see what is currently being audited:

- select * from dba_stmt_audit_opts;
- select * from dba_priv_audit_opts;
- select * from dba_obj_audit_opts;

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- To audit the SYSDBA activities, see MOS note 174340.1: Audit SYS user Operations. This additional SYS auditing can be enabled by setting the INIT.ORA parameter:

- AUDIT_SYS_OPERATIONS = TRUE.

- To audit activities of users who have the DBA role, determine which users have the DBA role, then activate auditing for those users:

- audit all privileges by <user> by access;

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- To audit the use of "…ANY…" privileges:
- Get a list of the "… ANY …" privileges:

```
select name from system_privilege_map
where name like '% ANY %';
```

- Enable auditing for the use of each of those privileges. Here is a SQL statement that will generate the appropriate AUDIT statements:

```
select 'audit ' || name || ';' sql_stmt
from system_privilege_map
where name like '% ANY %';
```

FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE

- To disable auditing for certain "… ANY …" privileges:

```
select 'noaudit ' || name || ';' sql_stmt
from system_privilege_map
where name like '% ANY %';
```

PUBLIC PRIVILEGES

- “The topic of PUBLIC privileges is part of Oracle's overall secure-by-default initiative that started with Oracle Database 9i. New in the Oracle Database 11g release are granular authorizations for numerous PL/SQL network utility packages granted to PUBLIC. If you have upgraded from a previous release of Oracle Database, and your applications depend on PL/SQL network utility packages such as UTL_TCP, UTL_SMTP, UTL_MAIL, UTL_HTTP AND UTL_INADDR the following error may occur when you try to run the application:

PUBLIC PRIVILEGES

- **METRIC: Execute permission for UTL_ networking packages has been revoked from PUBLIC.**
- **METRIC: UTL_FILE_DIR does not include any wildcards.**
- **METRIC: UTL_FILE_DIR does not include sensitive or protected directories.**
- **METRIC: The UTL_FILE_DIR init.ora parameter is not used.**
- **METRIC: UTL_FILE access is controlled via DIRECTORY objects.**

PUBLIC PRIVILEGES

- HOW TO CHECK:

```
select * from dba_tab_privs
where table_name in
('UTL_TCP','UTL_SMTP','UTL_INADDR','UTL_HTTP','UTL_MAIL'
)
and grantee = 'PUBLIC';
```

- This should return no rows.

PUBLIC PRIVILEGES

- show parameter utl_file_dir
- The value of this INIT.ORA parameter should be blank.
- select * from dba_directories;
- This should return rows.

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

- When granting permissions on run-time facilities such as the Oracle Java Virtual Machine (OJVM), grant permissions to the explicit or actual document root file path. This code can be changed to use the explicit file path.

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

- dbms_java.grant_permission ('SCOTT','SYS:java.io.FilePermission','<<ALL FILES>>','read');

- dbms_java.grant_permission ('SCOTT','SYS:java.io.FilePermission','<<actual directory path>>','read');

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

- **METRIC: Additional File I/O runtime privileges for Java use specific directory paths.**

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

- HOW TO CHECK:

- select * from dba_java_policy
- where type_name like '%File%';

RESTRICT PERMISSIONS ON RUN-TIME FACILITIES

- There are also Java permissions for network access. Here is a SQL statement that shows the existing Java permissions:

```
select * from dba_java_policy
where type_name like '%Socket%';
```

- As an increased security measure, DBAs may wish to restrict these Java permissions also.

AUTHENTICATE CLIENTS

- “Oracle recommends verifying that the database initialization parameter REMOTE_OS_AUTHENT is set to FALSE. Setting the value to FALSE creates a more secure configuration by enforcing server-based authentication of clients connecting to an Oracle database. The default setting for this parameter is FALSE and it should not be changed.”

AUTHENTICATE CLIENTS

- **METRIC: INIT.ORA parameter remote_os_authent is FALSE.**

AUTHENTICATE CLIENTS

- HOW TO CHECK:

- show parameter remote_os_authent

RESTRICT OPERATING SYSTEM ACCESS

- “Limit the number of users with operating system access on the Oracle Database host. Oracle recommends restricting the ability to modify the default file and directory permissions for the Oracle Database home (installation) directory or its contents. Even privileged operating system users and the Oracle owner should not modify these permissions, unless instructed otherwise by Oracle.

RESTRICT OPERATING SYSTEM ACCESS

- Restrict usage of symbolic links on the operating system. When providing a path or file to the Oracle database, neither the file nor any part of the path should be modifiable by an un-trusted user. The file and all components of the path should be owned by the DBA or another trusted operating system account."

RESTRICT OPERATING SYSTEM ACCESS

- **METRIC: Number of users with OS access to database server is limited.**
- **METRIC: Restrict OS-level access to files with sensitive content.**
- **METRIC: Files underneath $ORACLE_HOME can only be modified by DBAs.**
- **METRIC: Nodes above $ORACLE_HOME can only be modified by administrators.**

RESTRICT OPERATING SYSTEM ACCESS

- **METRIC: Components of file paths to database files are only modifiable by a trusted user.**
- **METRIC: Components of file paths to database files are owned by a trusted user.**
- **METRIC: Use of symbolic links is restricted.**

RESTRICT OPERATING SYSTEM ACCESS

- HOW TO CHECK:

- Review /etc/passwd with the DBA, to ensure that the number of users with OS level access is limited.

RESTRICT OPERATING SYSTEM ACCESS

- Scripts to check ownership and permissions of $ORACLE_HOME files:

- find $ORACLE_HOME ! -user oracle -print | xargs ls -ld
- find $ORACLE_HOME ! -group oinstall -print | xargs ls -ld
- find $ORACLE_HOME -perm -2 ! –type l -print | xargs ls -ld

RESTRICT OPERATING SYSTEM ACCESS

- Navigate up the filepath, and do an “ls -ld" to determine if the node is modifiable by untrusted personnel.

RESTRICT OPERATING SYSTEM ACCESS

- Ensure that the database datafiles are not readable by persons with non-DBA privileges.

```
select name from v$controlfile
union select member from v$logfile
union select name from v$datafile
union select name from v$tempfile;
```

- Then, examine the ownership and permissions on the individual files.

SECURE THE ORACLE LISTENER

- “The Oracle Listener should be properly configured for optimal security. Oracle Database 10g Release 1 and higher uses local OS authentication as the default authentication mode. This mode requires the Oracle Net administrator to be a member of the local DBA group.

SECURE THE ORACLE LISTENER

- You should also consider using a firewall. Proper use of a firewall will reduce exposure to security related information including port openings and other configuration information located behind the firewall. Oracle Net supports a variety of firewalls."

SECURE THE ORACLE LISTENER

- **METRIC: Listeners prior to 10g have access controlled via a password.**
- **METRIC: Listeners 10g or later do not have a password.**
- **METRIC: Firewalls are used to limit SQL*Net connections from trusted clients only**

SECURE THE ORACLE LISTENER

- HOW TO CHECK:
- Run:
  - lsnrctl status
- Look for:
  - Security ON: Local OS Authentication

SECURE THE ORACLE LISTENER

- “The default configuration for external procedures no longer requires a network listener to work with Oracle Database and EXTPROC agent. The EXTPROC agent is spawned directly by Oracle Database and eliminates the risks that extproc might be spawned by Oracle Listener, unexpectedly. This default configuration is recommended for maximum security.

SECURE THE ORACLE LISTENER

- Having your EXTPROC agent spawned by Oracle Listener is necessary if you use:
  - Multi-threaded Agent
  - Oracle Database in MTS mode on Windows
  - AGENT clause of the LIBRARY specification or AGENT IN clause of the PROCEDURE specification such that you can redirect external procedures to a different EXTPROC agent.

SECURE THE ORACLE LISTENER

- **METRIC: Listener configuration files do not have EXTPROC configured.**
- **METRIC: If EXTPROC functionality is required, is has been configured securely.**
- **METRIC: EXTPROC_DLLS=ONLY has been used instead of EXTPROC_DLLS=ALL.**
- **METRIC: A separate listener, running as an unprivileged user, is used for EXTPROC.**
- **METRIC: Audit who has the CREATE LIBRARY privileges**

SECURE THE ORACLE LISTENER

- HOW TO CHECK:
- Review the SQL*Net Listener configuration files:
  - Are EXTPROC entries present?
  - If so, is EXTPROC_DLLS=ONLY (used instead of EXTPROC_DLLS=ALL)?
  - Is EXTPROC functionality provided via a separate listener?
  - Is the separate listener running as an unprivileged user?

PREVENT RUNTIME CHANGES TO LISTENER

- “When the ADMIN_RESTRICTIONS_LISTENER is set to ON (Default) runtime changes to the listener parameters is disabled. To make changes, the LISTENER.ORA file must be modified and manually reloaded.”

PREVENT RUNTIME CHANGES TO LISTENER

- **METRIC: The SQL*Net Listener ADMIN_RESTRICTIONS parameter is set to ON.**

PREVENT RUNTIME CHANGES TO LISTENER

- HOW TO CHECK:
- Review the listener.ora file. You should see:
  - ADMIN_RESTRICTIONS_{listener name} = ON
- If it is not set, you can edit the listener.ora file manually.

CHECKING NETWORK IP ADDRESSES

- “Use the Oracle Net valid note checking security feature to allow or deny access to Oracle server processes from network clients with specified IP address. To use this feature, set the following protocol.ora (Oracle Net configuration file) parameters:
  - tcp.validnode_checking = YES
  - tcp.excluded_nodes = {list of IP addresses}
  - tcp.invited_nodes = {list of IP addresses}

CHECKING NETWORK IP ADDRESSES

- The first parameter turns on the feature whereas the latter parameters respectively deny or allow specific client IP address from making connections to the Oracle listener."

CHECKING NETWORK IP ADDRESSES

- **METRIC: SQL*Net valid node checking is used to limit access to the SQL*Net listener.**

CHECKING NETWORK IP ADDRESSES

- HOW TO CHECK:
- Review the $ORACLE_HOME/network/admin/sqlnet.ora file.
- See if these parameter are set.

CHECKING NETWORK IP ADDRESSES

- Oracle recommends limiting client connections from authorized clients only. This can be activated via the Database Access Control parameters (TCP.VALIDNODE_CHECKING, TCP.EXCLUDED_NODES, and TCP.INVITED_NODES). This configuration can be done using Oracle Net Manager.

CHECKING NETWORK IP ADDRESSES

- Resources:

- http://download.oracle.com/docs/cd/B19306_01/network.102/b14212/profile.htm#sthref868

- See MOS note 462933.1 ("What is Validnode Verification and How to Use It") for details.

HARDEN THE OPERATING SYSTEM

- "Both UNIX and Windows platforms provide a variety of operating system services, most of which are not necessary for most deployments. Such services include FTP, TFTP, TELNET and so forth. Be sure to close both the UDP and TCP ports for each service that is being disabled. Disabling one type of port and not the other does not make the operating system more secure."

HARDEN THE OPERATING SYSTEM

- **METRIC: Unencrypted UNIX services are disabled on the server**

HARDEN THE OPERATING SYSTEM

- HOW TO CHECK:

- Check which services are enabled on the server. For Unix, look at /etc/inetd.conf. This will tell you if any unencrypted services are enabled.

ENCRYPT NETWORK TRAFFIC

- “Consider encrypting network traffic between clients, databases and application servers. Oracle supports both SSL using X.509v3 certificates as well as native network encryption without certificates.”

ENCRYPT NETWORK TRAFFIC

- **METRIC: SQL*Net traffic is encrypted**

ENCRYPT NETWORK TRAFFIC

- Where do the special SQL*Net values go?
  - Server-side values go in listener.ora
  - Client-side values go in sqlnet.ora

ENCRYPT NETWORK TRAFFIC

- TRACE_LEVEL_ORCL = OFF
- #### TRACE_LEVEL_ORCL = SUPPORT
- SQLNET.ENCRYPTION_SERVER = REQUESTED
- SQLNET.CRYPTO_CHECKSUM_SERVER = REQUESTED
- SQLNET.ENCRYPTION_CLIENT=REQUESTED
- SQLNET.CRYPTO_CHECKSUM_CLIENT=REQUESTED

ENCRYPT NETWORK TRAFFIC

- TRACE_LEVEL_CLIENT = OFF
- TRACE_LEVEL_SERVER = OFF
- #### TRACE_LEVEL_CLIENT = SUPPORT
- #### TRACE_LEVEL_SERVER = SUPPORT
- SQLNET.ENCRYPTION_SERVER=REQUIRED
- SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED
- SQLNET.ENCRYPTION_CLIENT=REQUIRED
- SQLNET.CRYPTO_CHECKSUM_CLIENT=REQUIRED

APPLY ALL SECURITY PATCHES

- “Always apply relevant security patches for both the operating system and Oracle. Periodically check the Oracle Technology Network (OTN) security site for details on security alerts released by Oracle. Also check Oracle Worldwide Supports services site, MOS, for detailed on available and upcoming security related patches and application specific secure configuration information.”

APPLY ALL SECURITY PATCHES

- **METRIC: The latest CPU security patches are applied in a timely fashion.**

APPLY ALL SECURITY PATCHES

- HOW TO CHECK:

- Use “opatch lsinventory” to get a list of patches that have been applied, and look up those patches on MOS. Then, you will know which patches have been applied.

REPORT SECURITY ISSUES TO ORACLE

- “If you believe that you have found a security vulnerability in the Oracle Database, submit an service request to Oracle Worldwide Support Services using MOS, or email a complete description of the problem including product version and platform, together with any scripts and examples to the following address:
  - secalert_us@oracle.com”

REPORT SECURITY ISSUES TO ORACLE

- **METRIC: If the DBAs find a security vulnerability, they report it to Oracle.**

QUESTIONS AND ANSWERS

JIBE