In-Source Your IT Audit Series

How to Audit the Top Ten E-Business Suite Security Risks

February 28, 2012

Jeffrey T. Hare, CPA CISA CIA
Industry Analyst, Author, Consultant
ERP Risk Advisors

Stephen Kost
Chief Technology Officer
Integrigy Corporation
Speakers

Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- Founder of ERP Risk Advisors / ERP Seminars and Oracle User Best Practices Board
- 14 years working with Oracle EBS as client and consultant
- Experience includes Big 4 audit, 6 years in CFO/Controller roles – both as auditor and auditee
- Author – *Oracle E-Business Suite Controls: Application Security Best Practices*

Stephen Kost
Integrigy Corporation

- CTO and Founder
- 16 years working with Oracle and 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, ...
- Integrigy Consulting – Oracle EBS security assessments and services
- Integrigy AppSentry – Oracle EBS Security Assessment and Audit
About Integrigy

**ERP Applications**
Oracle E-Business Suite

**Products**

**AppSentry**
ERP Application and Database Security Auditing Tool

**AppDefend**
Enterprise Application Firewall for the Oracle E-Business Suite

**Services**

**Security Assessments**
ERP, Database, Sensitive Data, Pen Testing

**Compliance Assistance**
SOX, PCI, HIPAA

**Security Design Services**
Auditing, Encryption, DMZ

You
Agenda

1. Risks, Threats, and Vulnerabilities
   - Passwords

2. Internal and External Access
   - Controls, Policies, and Procedures

3. Q&A
Top 10 Security Vulnerabilities

1. Default Database Passwords
2. Default Application Passwords
3. Direct Database Access
4. Poor Application Security Design
5. External Application Access Configuration
6. Poor Patching Policies and Procedures
7. Access to SQL Forms in Application
8. Weak Change Control Procedures
9. No Database or Application Auditing
10. Weak Application Password Controls
## Significant Security Risks and Threats

<table>
<thead>
<tr>
<th>Risks and Threats</th>
<th>1 DB Pass</th>
<th>2 App Pass</th>
<th>3 Direct Access</th>
<th>4 App Sec Design</th>
<th>5 Extern App</th>
<th>6 Patch Policy</th>
<th>7 SQL Forms</th>
<th>8 Change Control</th>
<th>9 Audit</th>
<th>10 Pass Control</th>
</tr>
</thead>
</table>
| - Bulk download via direct access  
| - Update a bank account number  
| - Bypass intended app controls  
| - Wipe out the database  
Oracle E-Business Suite database is delivered with up to 300 database accounts:
- Default passwords (GL = GL)
- Active
- Significant privileges
# Default Oracle Password Statistics

<table>
<thead>
<tr>
<th>Database Account</th>
<th>Default Password</th>
<th>Exists in Database %</th>
<th>Default Password %</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>CHANGE_ON_INSTALL</td>
<td>100%</td>
<td>3%</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>MANAGER</td>
<td>100%</td>
<td>4%</td>
</tr>
<tr>
<td>DBSNMP</td>
<td>DBSNMP</td>
<td>99%</td>
<td>52%</td>
</tr>
<tr>
<td>OUTLN</td>
<td>OUTLN</td>
<td>98%</td>
<td>43%</td>
</tr>
<tr>
<td>MDSYS</td>
<td>MDSYS</td>
<td>77%</td>
<td>18%</td>
</tr>
<tr>
<td>ORDPLUGINS</td>
<td>ORDPLUGINS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>ORDSYS</td>
<td>ORDSYS</td>
<td>77%</td>
<td>16%</td>
</tr>
<tr>
<td>XDB</td>
<td>CHANGE_ON_INSTALL</td>
<td>75%</td>
<td>15%</td>
</tr>
<tr>
<td>DIP</td>
<td>DIP</td>
<td>63%</td>
<td>19%</td>
</tr>
<tr>
<td>WMSYS</td>
<td>WMSYS</td>
<td>63%</td>
<td>12%</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>CTXSYS</td>
<td>54%</td>
<td>32%</td>
</tr>
</tbody>
</table>

* Sample of 120 production databases
How to Check Database Passwords

1. Use Oracle’s **DBA_USERS_WITH_DEFPWD**
   - Limited set of accounts
   - Single password for each account

2. Command line tools (orabf, etc.)
   - Difficult to run – command line only

3. AppSentry
   - Checks all database accounts
   - Uses passwords lists -> 1 million passwords
   - Allows custom passwords
Seeded Application Accounts

- Oracle EBS delivered with up to 40 seeded application accounts
- Most seeded applications have default passwords
- Some accounts are active
- Some accounts have significant privileges
# Seeded Application Account Responsibilities

<table>
<thead>
<tr>
<th>Active Application Account</th>
<th>Default Password</th>
<th>Active Responsibilities</th>
</tr>
</thead>
</table>
| **ASGADM**                 | WELCOME          | ▪ SYSTEM_ADMINISTRATOR  
                          |                  | ▪ ADG_MOBILE_DEVELOPER |
| **IBE_ADMIN**              | WELCOME          | ▪ IBE_ADMINISTRATOR     |
| **MOBADM**                 | MOBADM           | ▪ MOBILE_ADMIN          
                          |                  | ▪ SYSTEM_ADMINISTRATOR |
| **MOBILEADM**              | WELCOME          | ▪ ASG_MOBILE_ADMINISTRATOR 
                          |                  | ▪ SYSTEM_ADMINISTRATOR |
| **OP_CUST_CARE_ADMIN**    | OP_CUST_CAREADMIN| ▪ OP_CUST_CARE_ADMIN    |
| **OP_SYSADMIN**            | OP_SYSADMIN      | ▪ OP_SYSADMIN           |
| **WIZARD**                 | WELCOME          | ▪ AZ_ISETUP             
                          |                  | ▪ APPLICATIONS FINANCIALS  
                          |                  | ▪ APPLICATION IMPLEMENTATION |
How to Check Applications Passwords

1. Decrypt all passwords
   - Google: oracle applications password decryption

2. Login to each account
   - Need to manually test 25 – 40 accounts

3. AppSentry
   - Checks all seeded application account passwords for default or weak passwords
   - Checks all seeded application accounts are locked
Direct Database Access

- Database access is a key problem
  - APPS_READ
  - Read only accounts often created with read to all data

- Access to sensitive data by generic accounts
  - Granularity of database privileges, complexity of data model, and number of tables/views make it difficult to create limited privilege database accounts
  - Must use individual database accounts with roles limiting access to data along with other security
How to Review Direct Database Access

1. Need to review who is accessing the database
   - Must have auditing enabled to determine generic database access

2. No standard method to review database privileges
   - Must manually review database privileges
   - Need to understand data model to know what can be accessed with granted privileges
Oracle EBS installs all modules (250+) and **all web pages** for every application server.

- All web pages access the database using the **APPS** database account.
Oracle EBS DMZ Certified Modules (R12)

Oracle only certifies a limited set of modules for use in a DMZ

- Meets DMZ architectural requirements (i.e., no forms)
- URL Firewall rules provided for the module

iSupplier Portal (POS)
Oracle Sourcing (PON)
Oracle Receivables (OIR)
iRecruitment (IRC)
Oracle Time and Labor (OTL)
Oracle Learning Management (OTA)
Self Service Benefits (BEN)
Self Service Human Resources (SSHR)
Oracle iSupport (IBU)
Oracle iStore (IBE)
Oracle Marketing (AMS)
Oracle Partner Relationship Mgmt (PRM)
Oracle Survey (IES)

Oracle Transportation (FTE)
Oracle Contracts Core (OKC)
Oracle Service Contracts (OKS)
Oracle Collaborative Planning (SCE)
Oracle User Management (UMX)
Order Information Portal (ONT)
Oracle Sales for Handhelds (ASP)
Oracle Internet Expenses (OIE)
Oracle Performance Management (OPM)
Compensation Workbench (CWB)
Oracle Payroll (PAY)
Oracle Quoting (QOT)
Oracle Field Service 3rd Party Portal (FSE)
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided My Oracle Support (MOS) Note must be followed.

**380490.1** Oracle E-Business Suite R12 Configuration in a DMZ

**287176.1** DMZ Configuration with Oracle E-Business Suite 11i
How to Check the External Configuration

1. Review DMZ web architecture
   - SSL
   - Network firewall
   - Reverse proxy
   - Web application firewall (Integrigy’s AppDefend)
   - Load balancing and caching

2. Perform a penetration test?

3. Review URL firewall configuration

   - Review 8 major configuration steps

5. Configuration Review - AppSentry
   - Automates checking 6 of 8 major configuration steps
Forms that Allow SQL Statements

- Allow ad-hoc SQL statements to be executed within them (over 30 forms)
- Could be used to update high risk data such as supplier addresses and bank accounts
- May not have any audit trail (before/after values) created to know who made the update
- Examples include:
  - Alerts
  - Collection Plans
Forms that Allow SQL Statements

- Applications
- Attribute Mapping
- Attribute Mapping Details
- Audit Statements
- Business Rule Workbench
- Create QuickPaint Inquiry
- Custom Stream Advanced Setup
- Defaulting Rules
- Define Assignment Set
- Define Data Group
- Define Data Stream
- Define Descriptive Flexfield Segments
- Define Dynamic Resource Groups
- Define Function
- Define Pricing Formulas
- Define Pricing Formulas
- Define Security Profile
- Define Validation Templates
- Define Value Set
- Define WMS Rules
- Dynamic Trigger Maintenance
- Foundation Objects
- PL/SQL tester
- QA - Collection Plan Workbench
- Register Oracle IDs
- SpreadTable Diagnostics Form
- Spreadtable Metadata Administration
- Workflow Activity Approval Configuration Framework
- Workflow Process Configuration Framework
- Write Formula

... and others as released by Oracle
How to Check SQL Forms Access

- Sensitive function review
  - Difficult to do without an “SoD” tool – all of which can analyze access to high-risk single functions such as SQL forms
  - Look for high risk seeded responsibility usage such as:
    - Application Developer
    - Alert Manager
    - Quality
1. **Password Profile Options**
   - **Length, reuse, case, and failure limit** are System Profile Options
   - Password expiration time set for individual accounts

2. **Password operational procedures**
   - Initial passwords and password resets
   - Default methods in 11i and R12 weak
   - Improved in R12 with User Management (UMX)

3. **Secure Password Storage**
   - Allows decryption of account passwords
   - Not enabled by default
## Application Password Settings

<table>
<thead>
<tr>
<th>System Profile Options</th>
<th>11i Default</th>
<th>R12 Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signon Password Failure Limit</td>
<td>(null)</td>
<td>10</td>
</tr>
<tr>
<td>Signon Password Hard To Guess</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>(1 letter, 1 number, no repeating characters, not username)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signon Password Length</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Signon Password No Reuse</td>
<td>(null)</td>
<td>(null)</td>
</tr>
<tr>
<td>Signon Password Case</td>
<td>insensitive</td>
<td>insensitive</td>
</tr>
</tbody>
</table>

Signon Password settings must be changed to meet organization’s password policy.
Oracle EBS Password Decryption

- Oracle EBS end-user application passwords stored **encrypted**, not **hashed**
  - Account passwords stored in **FND_USER** table
  - Procedure to decrypt passwords well documented and published on the Internet
  - Google: oracle applications password decryption

- Secure hashing of passwords is **optional** and must be enabled by DBA
  - **Not enabled by default even in R12**
  - See Integrigy whitepaper for recommendations
How to Check Password Controls

1. Manual Review
   - Validate signon System Profile Options
   - Query all users by querying FND_USER table where PASSWORD_LIFESPAN_DAYS <> xx days
   - Check password encryption patch by querying FND_USER table
   - Review application account creation and password reset workflows with administrator

2. AppSentry
   - Checks signon System Profile Options against organization’s password security policy
   - Checks password encryption patch is enabled
AppSentry
Oracle Applications Password Failure Limit

Summary
'Signon Password Failure Limit' is against policy

Details
'Signon Password Failure Limit' profile option is not set (default is disabled) compared to a policy of 4. Change this profile option under System Administrator > Profile > System.

Target: Oracle Applications

Description
Number of unsuccessful login attempts before the account is locked. This feature is enabled by the system profile option "Signon Password Failure Limit" (SIGNON_PASSWORD_FAILURE_LIMIT). The default is to disable this feature.

This profile option is introduced by Oracle Patch 2061872, also available in Mini Pack 11i.FND.E.

Solution
Change the profile option "Signon Password Failure Limit" to the appropriate value using the System Administrator Responsibility. The recommended value is at least 3.
Jeff’s Conclusions

- Most of the vulnerabilities and risks are on-going whereas most audit processes are ‘point in time’
- Auditors need to recommend continuous controls monitoring related to these risks and audit the CCM, rather than point in time.
- Solutions such as AppSentry are preferable to manual solutions because they integrate all tests into a single User Interface and are updated as changes are made to the applications and technology stack.
Steve’s Conclusions

- Oracle E-Business Suite security and compliance requires a team effort
  - DBAs, IT Security and Internal Audit must work together to ensure a secure and compliant environment

- Security is constantly changing due to application changes and new risks
  - Periodic reviews and assessments are required

- No “silver bullet” exists for protecting the Oracle EBS
  - A combination of policies, procedures, reviews, and tools must be put in place to address this complex environment

- Adhere to the Oracle Best Practices for Oracle EBS security
  - See My Oracle Support Notes 189367.1 and 403537.1
  - Written by Integrigy
  - Oracle has not updated since 2007
References and Resources

- Integrigy’s Website
  - www.integrigy.com
  - Oracle E-Business Suite Security Whitepapers

- ERP Risk Advisors Oracle Internal Controls and Security List Server
  - http://groups.yahoo.com/group/OracleSox

- ERP Risk Advisors Internal Controls Repository
  - http://tech.groups.yahoo.com/group/oracleappsinternalcontrols

- Jeff’s Book

- Oracle Best Practices for Securing Oracle EBS
  - Metalink Note IDs 189367.1 and 403537.1 (“Best Practices“)
  - Metalink Note IDs 380490.1 and 287176.1 (DMZ config)
Contact Information

Jeffrey T. Hare
Industry Analyst, Author
ERP Risk Advisors
web: www.erpra.net
e-mail: jhare@erpra.net
linkedin: http://www.linkedin.com/in/jeffreythare

Stephen Kost
Chief Technology Officer
Integrigy Corporation
web: www.integrigy.com
e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog