Hidden Security Threats in Oracle E-Business Suite

March 14, 2013

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

Stephen Kost
Chief Technology Officer
Integrigy Corporation
Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- Founder of ERP Risk Advisors 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 14 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

**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
1. Application Password Decryption Threat
2. User Profile Options
3. Application Diagnostics
4. Sensitive Admin Page Access
5. Database Account Passwords

Conclusion
Application user passwords may be decrypted and multiple other user accounts may be used to circumvent application controls.

1. Read application passwords encrypted in FND_USER table (cloned from production)
2. Decrypt application passwords using published SQL statements
3. Login as ANY user using passwords decrypted from test/development

Live passwords during clones
### Oracle EBS Password Encryption

#### FND_USER Table

<table>
<thead>
<tr>
<th>USER_NAME</th>
<th>ENCRYPTED FOUNDATION_PASSWORD</th>
<th>ENCRYPTED_USER_PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUEST</td>
<td>ZG6EBD472D1208B0CDC78D7EC7730F9B249496F825E761BA3EB2FEBB54F6915FADA757EF4558CF438CF55D23FE32BE0BE52E</td>
<td>ZG6C08D49D524A1551A3068977328B1AFD26040FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06</td>
</tr>
<tr>
<td>SYSADMIN</td>
<td>ZH39A396EDCA4CA7C8D5395D94D8C915510C0C90DA198EC9CDA15879E8B547B9CDA034575D289590968F1B6B38A1E654DD98</td>
<td>ZHF57EAF37B1936C56755B134DE7C83AE40CADD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C8788</td>
</tr>
<tr>
<td>WIZARD</td>
<td>ZG2744DCFCCFFA381B994D2C3F7ADACF68DF433BADF59CF6C3DAB3C35A11AAAB2674C2189DCA040C4C81D2CE41C2BB82BFC6</td>
<td>ZGE9AA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8FE4451</td>
</tr>
</tbody>
</table>

#### Diagram

- **APPs password encrypted user name + user password**
- **User password encrypted using APPS password**
SELECT
    (SELECT get_pwd.decrypt (UPPER
        ((SELECT UPPER (fnd_profile.VALUE
            ('GUEST_USER_PWD')) FROM DUAL)),
        fu.encrypted_foundation_password)
    FROM DUAL) AS apps_password
FROM fnd_user fu
WHERE fu.user_name LIKE UPPER
    ((SELECT
        SUBSTR (fnd_profile.VALUE ('GUEST_USER_PWD') ,1 ,
        INSTR (fnd_profile.VALUE ('GUEST_USER_PWD'), '/') - 1 )
    FROM DUAL))
Oracle EBS Password Decryption

- Application passwords by default are encrypted, not hashed which is more secure
  Simple method to decrypt if able to access FND_USER table

- Secure hashing of passwords is optional and must be enabled by DBA
  Patch for earlier 11i versions and included with R12 but disabled by default

- Encrypted application passwords are cloned to test and development databases
  See Integrigy whitepaper for recommendations
Password Decryption Recommendations

- **Be sure password hashing is enabled by DBAs**
  DBAs must run FNDCPASS USERMIGRATE (MOS ID 457166.1)
  Verify it has been run successfully for all user (MOS ID 1084956.1)

- **Change all application user passwords when cloning from production to test and development**
  All environment credentials should be changed during clones
  Enable forgot password functionality for accessing passwords

- **Enable strong application password controls in all Oracle EBS environments**
  Prevents possible brute forcing of application password hashes
Agenda

1. Application Password Decryption Threat
2. User Profile Options
3. Application Diagnostics
4. Sensitive Admin Page Access
5. Database Account Passwords

Conclusion
Profile Options can be set through the System Profile Values form:
Profile Options can also be set through the User Profile Values form:
User Profile Values

- Risks:
  - Override of controls via the User Profile Values form
  - Changes to System Profile Options that are not analyzed / approved by appropriate personnel
  - System profile options are not set to meet control objectives or operational objectives – which may be in conflict
User Profile Values

- 8907 profile options in this R12 instance
User Profile Values

Example:

- **Profile Name:** GL Journal Review Required
- **Description:** Journal review required before posting
- **Hierarchy Type:** Security

### SQL Validation

SQL used for the Profile Option's List of Values:

```sql
SQL = "SELECT MEANING ("Journal review required"),
     LOOKUP_CODE
     INTO :visible_option_value,
     :profile_option_value
     FROM fnl_lookups
     WHERE lookup_type = "YES_NO"
     COLUMN="Journal review required"(30)"
```
User Profile Values

- **Example:**

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Default Value</th>
<th>User Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>GL: Journal Review Required</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
User Profile Values

- Control expectations – user profile values:
  - Access to the form is totally removed or
  - Personalization is done to restrict access to just those profile options that are low risk
User Profile Values

- Control expectations - overall:
  - A risk assessment has been performed to identify which profile options should be subject to the change management process, or all profile option changes are subject to the change management process
  - The change management documentation clearly identifies the profile options that are subject to the change management process or states that all profile option changes are subject to the change management process
User Profile Values

- Control expectations - overall:
  - A log-based or trigger-based auditing solution has been deployed to build a detailed audit trail of profile option changes.
  - A quality assurance process is in place that tests for unauthorized changes by tracing actual changes back to approved changes.
  - Testing of the change management process is performed to verify that the procedures have been followed and properly documented – approvals obtained, etc.
Application Diagnostics

- Represents ‘back door’ access to tables
- Enabled through Utilities: Diagnostics profile option
Risks:
- Back door access to maintain data not visible through forms such as IDs
- Corruption of data
Application Diagnostics

- Risks: Back door access to maintain data not visible through forms such as IDs
Application Diagnostics

- Example – before:
Application Diagnostics

- Example – change made:
Application Diagnostics

- Example – after:
Application Diagnostics

- **Recommendations:**
  - Do not allow in Prod for ANYONE other than those that already have access to the APPS password.
  - See more recommendations related to profile options in earlier section on profile options.
Some **forms** and **pages** in Oracle E-Business Suite allow a user to modify the functionality of the applications by specifying values such as **SQL statements**, **SQL fragments** such as WHERE clauses, **HTML strings**, and **operating system commands** or environment variables.
Non-privileged users may be able to execute SQL as the APPS database account or operating system commands as the database owner.

1. Enters malicious SQL statement into form or page inadvertently granted (for example Oracle Alerts)
2. Oracle EBS executes SQL statement as APPS database account
3. SQL changes SYSADMIN password and allows unauthorized login
Forms that Allow SQL *(Partial Listing)*

- 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
- 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
Sensitive Administrative Pages

- Sensitive forms and pages often not given appropriate emphasis in SOD matrices
  Review SOD matrices to verify all functions are listed

- Oracle listings of sensitive forms and pages are not complete due to the complexity of the application
  Very difficult to identify every possible form and page

- User access at the function level must be reviewed to identify privilege violations
  Use Oracle provided SQL script to get a listing of function access
Agenda

Introduction

1. Application Password Decryption Threat
2. User Profile Options
3. Application Diagnostics
4. Sensitive Admin Page Access
5. Database Account Passwords

Conclusion
Default or weak database passwords may allow unauthorized access to the database. Almost every database account can have privileged access.

**Threat**

1. Read database password hashes from user$ (cloned from production)
2. Brute force* password hashes at home over the weekend or for a month
3. Login as using brute forced password from test/development

*Google: oracle password cracker
Oracle Database password algorithm published

- Oracle 11g – hash changed to SHA-1 – old DES hash also stored

Hash is unique to the username, but common across all versions and platforms of the Oracle database

- SYSTEM/MANAGER is always D4DF7931AB130E37 in every Oracle database in the world

Database password hashes cloned to development
300+ database accounts by default
- One account for each module (GL=GL) and a few extras (APPS)
- Default password for almost all accounts is the username

Every EBS database account has significant privileges

A new database account is added for each new product module during an upgrade or patching
- R12.1 upgrade = CA, DDR, DNA, DPP, FTP, GMO, IBW, INL, IPM, ITA, JMF, MTH, PFT, QPR, RRS, ...
## 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>ORDPLUGIN</td>
<td>ORDPLUGIN</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
A number of efficient password brute forcing programs exist for Oracle
- Speed is at least 1 million passwords per second for desktop/laptop
- Speed is around 100 million passwords per second for specialized hardware (FGPA/GPU)
- Only the username and hash are required
- Estimated time to brute force a password of x length -

<table>
<thead>
<tr>
<th>Length</th>
<th>Permutations</th>
<th>Time (desktop)</th>
<th>Time (GPU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26 (26)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>2</td>
<td>1,040 (26 x 39)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>3</td>
<td>40,586 (26 x 39 x 39)</td>
<td>0 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>4</td>
<td>1,582,880</td>
<td>1.5 seconds</td>
<td>0 seconds</td>
</tr>
<tr>
<td>5</td>
<td>61,732,346</td>
<td>2 minute</td>
<td>6 seconds</td>
</tr>
<tr>
<td>6</td>
<td>2,407,561,520</td>
<td>40 minutes</td>
<td>24 seconds</td>
</tr>
<tr>
<td>7</td>
<td>93,894,899,306</td>
<td>1 day</td>
<td>15 minutes</td>
</tr>
<tr>
<td>8</td>
<td>3,661,901,072,960</td>
<td>42 days</td>
<td>10 hours</td>
</tr>
<tr>
<td>9</td>
<td>142,814,141,845,466</td>
<td>1,600 days</td>
<td>16 days</td>
</tr>
</tbody>
</table>
How to Check Database Passwords

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

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

- **AppSentry**
  - Checks all database accounts
  - Uses passwords lists - > 1 million passwords
  - Allows custom passwords
Conclusions

- Security is complicated, not a one-time event, and ever-changing
- Oracle’s security documents cannot be relied upon as complete
Upcoming Webinars

Sensitive Administrative Pages in Oracle EBS: Are You Overlooking This Threat
Wednesday, April 24th, 2013
2:00pm EDT
www.integrity.com/upcoming-events

Oracle EBS Account Password Decryption Threat Explored
Thursday, May 23rd, 2013
2:00m EDT
www.integrity.com/upcoming-events
<table>
<thead>
<tr>
<th>Resources</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrigy’s Website</strong></td>
<td><a href="http://www.integrigy.com">www.integrigy.com</a> Oracle EBS Security Whitepapers and Blog</td>
</tr>
<tr>
<td><strong>ERP Risk Advisors Oracle Internal Controls and Security List Server</strong></td>
<td><a href="http://groups.yahoo.com/group/OracleSox">http://groups.yahoo.com/group/OracleSox</a></td>
</tr>
<tr>
<td><strong>ERP Risk Advisors Internal Controls Repository</strong></td>
<td><a href="http://tech.groups.yahoo.com/group/oracleappsinternalcontrols">http://tech.groups.yahoo.com/group/oracleappsinternalcontrols</a></td>
</tr>
</tbody>
</table>
| **Oracle Support Security Notes (MOS)**         | Security Configuration | 189367.1 – 11i  
                                                      | 403537.1 – R12  
                                                      | DMZ Configuration | 287176.1 – 11i  
                                                      | 380490.1 – R12 |
Other Resources

- Recorded webinars at:

- Free 10,000 assessment from ERP Risk Advisors. Details at: www.erpra.net
Contact Information

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

**Stephen Kost**
Chief Technology Officer
Integrigy Corporation
web: [www.integrigy.com](http://www.integrigy.com)
e-mail: info@integrigy.com
blog: [integrigy.com/oracle-security-blog](http://integrigy.com/oracle-security-blog)
youtube: [youtube.com/integrigy](http://youtube.com/integrigy)