Internal Auditor Primer: Oracle E-Business Suite Security Risks Primer

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

December 9, 2010
Stephen Kost

- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, ...

Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool
# Integrigy Security Alerts

<table>
<thead>
<tr>
<th>Security Alert</th>
<th>Versions</th>
<th>Security Vulnerabilities</th>
</tr>
</thead>
</table>
| Critical Patch Update July 2008       | Oracle 11g 11.5.8 – 12.0.x | - 2 Issues in Oracle RDBMS Authentication  
                                        |                           | - 2 Oracle E-Business Suite vulnerabilities                                              |
| Critical Patch Update April 2008      | 12.0.x 11.5.7 – 11.5.10   | - 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.                    |
| Critical Patch Update July 2007       | 12.0.x 11.5.1 – 11.5.10   | - 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.                   |
| Critical Patch Update October 2005    | 11.5.1 – 11.5.10 11.0.x   | - Default configuration issues                                                           |
| Critical Patch Update July 2005       | 11.5.1 – 11.5.10 11.0.x   | - SQL injection vulnerabilities                                                           
                                        |                           | - Information disclosure                                                                 |
| Critical Patch Update April 2005      | 11.5.1 – 11.5.10 11.0.x   | - SQL injection vulnerabilities                                                           
                                        |                           | - Information disclosure                                                                 |
| Critical Patch Update Jan 2005        | 11.5.1 – 11.5.10 11.0.x   | - SQL injection vulnerabilities                                                           |
| Oracle Security Alert #68             | Oracle 8i, 9i, 10g        | - Buffer overflows  
                                        |                           | - Listener information leakage                                                           |
| Oracle Security Alert #67             | 11.5.1 – 11.5.8 11.0.x   | - 10 SQL injection vulnerabilities                                                       |
| Oracle Security Alert #56             | 11.5.1 – 11.5.8 11.0.x   | - Buffer overflow in FNDWRR.exe                                                           |
| Oracle Security Alert #55             | 11.5.1 – 11.5.8           | - Multiple vulnerabilities in AOL/J Setup Test  
                                        |                           | - Obtain sensitive information (valid session)                                           |
| Oracle Security Alert #53             | 10.7, 11.0.x 11.5.1 – 11.5.8 | - No authentication in FNDFS program  
                                        |                           | - Retrieve any file from O/S                                                            |
Agenda

1. Compliance Issues
   - Security Best Practices
2. Protection of Sensitive Data
3. Privileges and Access
4. Secure Remote Access

INTEGRIGY
Protection of Sensitive Data

Secure Remote Access

Compliance Issues

1. Security Best Practices

2. Privileges and Access

3. Privileges and Access

4. Privileges and Access

5. Privileges and Access
Security and Compliance Drivers

- **Sarbanes-Oxley (SOX)**
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets

- **Payment Card Industry - Data Security Standard (PCI-DSS)**
  - 12 stringent security requirements

- **Privacy (National/State Regulations)**
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - California and Massachusetts data privacy laws

- **Business Audit and Security Requirements**
  - Internal adoption of COBIT or COSO
  - Preventative and detective controls
# PCI-DSS – Compliance Effort

<table>
<thead>
<tr>
<th>#</th>
<th>Requirement</th>
<th>OS/Network</th>
<th>Oracle DB</th>
<th>Oracle EBS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Use Firewall to protect data</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Do not use vendor-supplied defaults</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Protect stored cardholder data</td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Encrypt across open, public networks</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Use Anti-virus software</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Develop and maintain secure applications</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>Restrict access to cardholder data</td>
<td></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>Assigned unique IDs for access</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>Restrict physical access to data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Track and monitor access</td>
<td>7</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>Regularly test security</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>Maintain information security policy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Colors:
- Red: High
- Orange: Medium
- Yellow: Low
Security and Compliance Drivers

- **Sarbanes-Oxley (SOX)**
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets

- **Payment Card Industry - Data Security Standard (PCI-DSS)**
  - 12 stringent security requirements

- **Privacy (National/State Regulations)**
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - California and Massachusetts data privacy laws

- **Business Audit and Security Requirements**
  - Internal adoption of COBIT or COSO
  - Preventative and detective controls
PCI-DSS Compliance Example

- PCI 6.1 – “Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.”

- Few Oracle customers install patches within 30 days
- Most customers are 1 to 2 quarters behind
- Business must prioritize applying security patches – effort to functionally test and apply, down-time

- See Integrigy Whitepaper “Oracle Applications 11i: Credit Cards and PCI Compliance Issues”
Agenda

1. Compliance Issues
2. Protection of Sensitive Data
4. Privileges and Access
5. Secure Remote Access
Database connectivity is a complex problem.

Your Oracle Database

- Ad-hoc Users
- Application
- Reporting Tools
- Batch Processing
- Interfaces and Feeds
- DBAs
- Application Admins
- Backup Tools
- Management Tools
Database security **decays** over time
Organizational Misalignment

- **IT Security**
  - Excellent at network and operating system security
  - Limit or no understanding of database security
  - Securing Oracle EBS is different than networks and operating systems
    - SQL, application architectures, data warehousing, etc.

- **Risk Management**
  - Database risk not properly quantified
  - Data classification not extended to caretaker of data
  - Databases and applications poor at handling data classification

- **Database Administrators (DBAs)**
  - Not aware of security requirements nor security-focused
  - No time to properly secure the database and application
  - Always afraid of impacting the application or performance of the database
## 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
Oracle CPU Patching Metric

Security Patches - Months Behind

- "n-1" patching standard
- No patches since last upgrade
- No patches and unsupported

Months

Production Databases
Key Security Risks

1. Exploitation of Oracle security vulnerabilities
   - Apply security patches
   - Limit direct connectivity to the database
   - Prohibit use of generic accounts by individuals

2. Brute forcing of Oracle database passwords
   - Limit access to password hashes
   - Change all database passwords in test and development

3. Decryption of Oracle EBS passwords
   - Apply latest Oracle EBS password patches
   - See Integriky whitepaper for recommendations
Oracle EBS Security Recommendations

- Adhere to the Oracle Best Practices for Oracle EBS security
  - See Metalink documents 189367.1 and 403537.1
  - Written by Integrigy
  - Oracle has not updated since 2007

- Perform periodic security reviews and assessment
  - Validate compliance against security best practices
Secure Remote Access

Compliance Issues

Protection of Sensitive Data

1. Security Best Practices
2. Privileges and Access
3. Protection of Sensitive Data
4. Privileges and Access
5. Secure Remote Access
Protecting Sensitive Data

- Database access is a key problem
  - APPS_READ

- All data duplicated in development and test databases
  - Data not always scrambled in non-production database

- Limited data encryption capabilities
  - No third-party encryption solutions work effectively
  - Oracle EBS only natively encrypts credit card numbers
  - Need to encrypt sensitive data on backup media

- Data and transaction retention policy
  - Oracle EBS is “data in” for life
  - Seldom data is purged or archived unless for performance
  - PCI Compliance = 1 to 2 years recommended retention
Key Data Protection Risks

1. Sensitive data accessible in test & development
   - All sensitive data must be scrambled in all non-production databases
   - Must periodically review database for instances of non-scrambled data as often in custom, interface, and temporary tables

2. 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
Oracle Credit Card Encryption

- Use the Oracle E-Business Suite encryption
  - Application-level encryption
  - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)

- Metalink Note ID 338756.1, Patch 4607647
  - Consolidates card numbers into IBY_SECURITY_SEGMENTS table
  - Encrypts card numbers in IBY_SECURITY_SEGMENTS
  - Uniform masking of card numbers
  - Significant functional pre-requisites (11.5.10.2)
Not pictured:
- Internet Expenses (AP) – R12
- Lease Management (AP) – same as AR
- Student System (IGS) – IGS patch
Agenda

1. Compliance Issues
2. Security Best Practices
3. Protection of Sensitive Data
4. Privileges and Access
5. Secure Remote Access
Privileges and Access in Oracle EBS

- Many generic and privileged accounts in application and database
  - Database - APPS, SYS, SYSTEM, APPLSYS, ...
  - Application - SYSTEM, GUEST
  - DBAs must use generic accounts for many maintenance activities
  - Generic application accounts used for scheduling key batch processes

- Database access is a key problem (Again)
  - Generic accounts are often used for ad-hoc database access
  - APPS_READ

- Limited auditing and control over the use of generic accounts
  - No auditing is enabled by default in database or application
  - Auditing on transactions often a major performance impact
Agenda

1. Compliance Issues
2. Protection of Sensitive Data
3. Secure Remote Access
4. Privileges and Access
5. Security Best Practices
External Access to Oracle EBS

- **Oracle EBS has certified “DMZ” modules for external access**
  - iStore, iSupplier, iSupport, iRecruitment, etc.
  - Only certified modules should be externally accessible

- **Oracle EBS never designed as a external web application**
  - All modules (250+) always installed
  - 40,000+ web pages are available even though not configured, licensed or used
  - If there is a security vulnerability, web application has access to all data
Key External Access Risks

1. Oracle EBS web architecture has inherent security weaknesses and deficiencies
   - Configuration for external is very specific and blocks access to major parts of the application
   - Must follow every step in Metalink documents 380490.1 (R12) and 287176.1 (11i)

2. Exploitation of Oracle security vulnerabilities
   - Risk is significantly different if Oracle EBS is externally accessible (internal network vs. world)
   - Firewalls and other security tools are ineffective
   - Application security patching is critical
Summary

- 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

- Security vulnerabilities must be addressed
  - The business must prioritize security patches

- 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
References and Resources

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

- **Oracle Best Practices for Securing Oracle EBS**
  - Metalink Note IDs 189367.1 and 403537.1

- **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 Hare’s Book**
  - *Oracle E-Business Suite Controls: Application Security Best Practices*

- **ISACA Book**
  - *Security, Audit and Control Features Oracle E-Business Suite*
Questions?
Integrigy Contact Information

Stephen Kost  
Chief Technology Officer  
Integrigy Corporation

e-mail: info@integrigy.com  
blog: integrigy.com/oracle-security-blog

For information on -

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

www.integrigy.com