Protecting Sensitive Data in Oracle E-Business Suite

February 28, 2013

Stephen Kost
Chief Technology Officer
Integrigy Corporation
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**
## Integrigy Published Security Alerts

<table>
<thead>
<tr>
<th>Security Alert</th>
<th>Versions</th>
<th>Security Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Critical Patch Update July 2011</strong></td>
<td>11.5.10 – 12.1.x</td>
<td>Oracle E-Business Suite security configuration issue</td>
</tr>
<tr>
<td><strong>Critical Patch Update October 2010</strong></td>
<td>11.5.10 – 12.1.x</td>
<td>2 Oracle E-Business Suite security weaknesses</td>
</tr>
<tr>
<td><strong>Critical Patch Update July 2008</strong></td>
<td>Oracle 11g 11.5.8 – 12.0.x</td>
<td>2 Issues in Oracle RDBMS Authentication, 2 Oracle E-Business Suite vulnerabilities</td>
</tr>
<tr>
<td><strong>Critical Patch Update April 2008</strong></td>
<td>12.0.x 11.5.7 – 11.5.10</td>
<td>8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</td>
</tr>
<tr>
<td><strong>Critical Patch Update July 2007</strong></td>
<td>12.0.x 11.5.1 – 11.5.10</td>
<td>11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</td>
</tr>
<tr>
<td><strong>Critical Patch Update October 2005</strong></td>
<td>11.0.x, 11.5.1 – 11.5.10</td>
<td>Default configuration issues</td>
</tr>
<tr>
<td><strong>Critical Patch Update July 2005</strong></td>
<td>11.5.1 – 11.5.10 11.0.x</td>
<td>SQL injection vulnerabilities, Information disclosure</td>
</tr>
<tr>
<td><strong>Critical Patch Update April 2005</strong></td>
<td>11.5.1 – 11.5.10 11.0.x</td>
<td>SQL injection vulnerabilities, Information disclosure</td>
</tr>
<tr>
<td><strong>Critical Patch Update Jan 2005</strong></td>
<td>11.5.1 – 11.5.10 11.0.x</td>
<td>SQL injection vulnerabilities</td>
</tr>
<tr>
<td><strong>Oracle Security Alert #68</strong></td>
<td>Oracle 8i, 9i, 10g</td>
<td>Buffer overflows, Listener information leakage</td>
</tr>
<tr>
<td><strong>Oracle Security Alert #67</strong></td>
<td>11.0.x, 11.5.1 – 11.5.8</td>
<td>10 SQL injection vulnerabilities</td>
</tr>
<tr>
<td><strong>Oracle Security Alert #56</strong></td>
<td>11.0.x, 11.5.1 – 11.5.8</td>
<td>Buffer overflow in FNDWRR.exe</td>
</tr>
<tr>
<td><strong>Oracle Security Alert #55</strong></td>
<td>11.5.1 – 11.5.8</td>
<td>Multiple vulnerabilities in AOL/J Setup Test, Obtain sensitive information (valid session)</td>
</tr>
<tr>
<td><strong>Oracle Security Alert #53</strong></td>
<td>10.7, 11.0.x 11.5.1 – 11.5.8</td>
<td>No authentication in FNDFS program, Retrieve any file from O/S</td>
</tr>
</tbody>
</table>
Controlling Data Access

Sensitive Data Overview

Encryption

Auditing

Q&A

1

2

3

4

5
Agenda

1. Sensitive Data Overview
2. Controlling Data Access
3. Encryption
4. Auditing
5. Q&A
Why - Security and Compliance Drivers

- 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)
  - Regulations often specifically exclude encrypted data
  - California (SB1386) and Massachusetts data privacy laws

- Sarbanes-Oxley (SOX)
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets
## What is Sensitive Data in Oracle EBS?

<table>
<thead>
<tr>
<th><strong>Payment Card Industry Data Security Standard (PCI-DSS 2.0)</strong></th>
<th><strong>State Privacy Regulations (employees, customers, Vendors)</strong></th>
<th><strong>HIPAA Privacy Standard/Rule</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Credit Card Number</td>
<td>▪ First and last name</td>
<td>▪ First and last name</td>
</tr>
<tr>
<td>▪ <strong>Primary Account Number (PAN)</strong></td>
<td>▪ Plus one of the following:</td>
<td>▪ Plus one of the following (Protected Health Information)</td>
</tr>
<tr>
<td>▪ CVV/CV2/CID</td>
<td>▪ Social security number</td>
<td>▪ “the past, present, or future physical or mental health, or condition of an individual”</td>
</tr>
<tr>
<td>▪ 3 digits on the back for Visa/MC</td>
<td>▪ Credit card number</td>
<td>▪ “provision of health care to an individual”</td>
</tr>
<tr>
<td>▪ 4 digits on the front for AMEX</td>
<td>▪ Bank account number</td>
<td>▪ “payment for the provision of health care to an individual”</td>
</tr>
<tr>
<td>▪ Magnetic Stripe Data (very rare)</td>
<td>▪ Financial account number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Driver license or state ID number</td>
<td></td>
</tr>
</tbody>
</table>

- **Payment Card Industry Data Security Standard (PCI-DSS 2.0)**
  - Credit Card Number
  - **Primary Account Number (PAN)**
  - CVV/CV2/CID
    - 3 digits on the back for Visa/MC
    - 4 digits on the front for AMEX
  - Magnetic Stripe Data (very rare)

- **State Privacy Regulations (employees, customers, Vendors)**
  - First and last name
  - Plus one of the following:
    - Social security number
    - Credit card number
    - Bank account number
    - Financial account number
    - Driver license or state ID number

- **HIPAA Privacy Standard/Rule**
  - First and last name
  - Plus one of the following (Protected Health Information)
    - “the past, present, or future physical or mental health, or condition of an individual”
    - “provision of health care to an individual”
    - “payment for the provision of health care to an individual”
<table>
<thead>
<tr>
<th>Where is Sensitive Data in Oracle EBS?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credit Card Data</strong></td>
</tr>
<tr>
<td>iby_security_segments (encrypted)</td>
</tr>
<tr>
<td>ap_bank_accounts_all</td>
</tr>
<tr>
<td>oe_order_headers_all</td>
</tr>
<tr>
<td>aso_payments</td>
</tr>
<tr>
<td>oks_k_headers_*</td>
</tr>
<tr>
<td>oks_k_lines_*</td>
</tr>
<tr>
<td>iby_trxn_summaries_all</td>
</tr>
<tr>
<td>iby_credit_card</td>
</tr>
<tr>
<td><strong>Social Security Number</strong></td>
</tr>
<tr>
<td>(National Identifier)</td>
</tr>
<tr>
<td>(Tax ID)</td>
</tr>
<tr>
<td>per_all_people_f</td>
</tr>
<tr>
<td>hr_h2pi_employees</td>
</tr>
<tr>
<td>ben_reporting</td>
</tr>
<tr>
<td>ap_suppliers</td>
</tr>
<tr>
<td>ap_suppliers_int</td>
</tr>
<tr>
<td>po_vendors_obs</td>
</tr>
<tr>
<td><strong>Bank Account Number</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>ap_checks_all</td>
</tr>
<tr>
<td>ap_invoice_payments_all</td>
</tr>
<tr>
<td>ap_selected_invoice_invoice_checks_all</td>
</tr>
<tr>
<td><strong>Protected Health Information (PHI)</strong></td>
</tr>
<tr>
<td>Order Management</td>
</tr>
<tr>
<td>Accounts Receivables</td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
</tbody>
</table>
Where else might be Sensitive Data?

**Custom tables**
- Customizations may be used to store or process sensitive data

**“Maintenance tables”**
- DBA copies tables to make backup prior to direct SQL update
- hr.per_all_people_f_011510

**Interface tables**
- Credit card numbers are often accepted in external applications and sent to Oracle EBS

**Oracle EBS Flexfields**
- It happens – very hard to find

**Interface files**
- Flat files used for interfaces or batch processing

**Log files**
- Log files generated by the application (e.g., iPayment)
How – EBS Data Protection Process

1. Enterprise Data Privacy Policy

2. Data Discovery and Design (Annually)
   - Detailed Data Inventory (element → table.column → action)

3. 
   - Native EBS Encryption (credit cards only)
   - Add-on Encryption (disk or database)
   - Database Access Controls
   - Auditing

4. Scrambling/Data Masking (Clone)

5. Security, Hardening, and General IT Controls

Production  Test/Development
## How - Data Protection vs. Threats

### Data Access Method and Threats

<table>
<thead>
<tr>
<th>Method and Threats</th>
<th>1 EBS Encrypt</th>
<th>2 Trigger View</th>
<th>3 Oracle TDE</th>
<th>4a FGAC</th>
<th>4b Internal Audit</th>
<th>4c External Audit</th>
<th>3 + 4 TDE + Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Application access by end-users (responsibility)</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>2. Application access by application administrators</td>
<td>E+</td>
<td>E-</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>3. Database access by DBA</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A+</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>4. Database access by Applications DBA (SYSTEM, APPS)</td>
<td>E+</td>
<td>E+</td>
<td></td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>5. Database access by other database accounts</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>6. Operating system access to database data files</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td>E</td>
</tr>
<tr>
<td>7. On-line or off-line access to database backups</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td>E</td>
</tr>
<tr>
<td>8. Exploitation of Oracle Applications security vulnerabilities</td>
<td>E-</td>
<td>E-</td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>9. Exploitation of Oracle Database security vulnerabilities</td>
<td>E+</td>
<td>E+</td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>10. Exploitation of operating system security vulnerabilities</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td>E</td>
</tr>
</tbody>
</table>

E = Encrypted,  C = Access Controlled,  A = Access Audited,  + = Mostly - = Partially
Types of Encryption

- **Storage (Data at rest)**
  - **Disk level encryption**
    - Encryption of data at rest such as when stored in files or on media

- **Access (Data in use)**
  - **Application or database level encryption**
    - Encryption of data with access permitted only to a subset of users in order to enforce segregation of duties

- **Network (Data in motion)**
  - Encryption of data when transferred between two systems
  - **SSL/HTTPS (users) and SQL*Net encryption (database)**
# Oracle EBS Encryption Solutions

| Application          | • Oracle EBS Credit Card Number Encryption  
|                      | • Encryption Customization (DBMS_CRYPTO/FND_VAULT) |
| (access = responsibility) |                          |
| Database             | • View/Trigger Encryption Solutions |
| (access = db account) |                          |
| Disk/Storage         | • Oracle Transparent Data Encryption (TDE)  
|                      | • Third-party Solutions (e.g., Vormetric)  
| (access = database)  | • Disk/SAN Vendor Encryption Solutions |
Native EBS Encryption (Credit Card Numbers)
Oracle Credit Card Encryption (no TDE)

- **Application-level encryption**
  - Not enabled by default in 11i or R12
  - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)
  - General patch release availability October 2006
  - Significant modification to application – 64 packages, 60 web pages, and 18 forms

- **11i** = MOS Note ID 338756.1, Patch 4607647
- **R12** = MOS Note ID 863053.1
  - 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
Oracle
Transparent Data Encryption (TDE)
What is Oracle TDE?

- **Transparent database encryption**
  - Requires no application code or database structure changes to implement
  - Only major change to database function is the Oracle Wallet must be opened during database startup
  - Add-on feature licensed with Advanced Security Option

- **Limited to encrypting only certain columns**
  - Cannot be a foreign key or used in another database constraint
  - Only simple data types like number, varchar, date, ...
  - Less than 3,932 bytes in length
What does TDE do and not do?

- TDE only encrypts “data at rest”

- TDE protects data if following is stolen or lost -
  - disk drive
  - database file
  - backup tape of the database files

- An authenticated database user sees no change

- Does TDE meet legal requirements for encryption?
  - California SB1386, Payment Card Industry Data Security
  - Ask your legal department
Data Center Theft

From Chicago Police Report -

- At least two masked intruders entered the suite after cutting into the reinforced walls with a power saw.
- During the robbery, the night manager was repeatedly tazed and struck with a blunt instrument.
- At least 20 data servers were stolen.
Column vs. Tablespace Encryption

**Column encryption**
- Fairly straightforward for simple cases such as `NATIONAL_IDENTIFIER` in `HR.PER_ALL_PEOPLE_F`
- Encryption done in place using `ALTER TABLE`
- Do not use SALT for Oracle EBS columns
- **Use for standard Oracle EBS columns**

**Tablespace encryption**
- Tablespace encryption only supported in 11g for 11i/R12
- Tablespace must be exported and imported to implement encryption
- OATM uses large tablespaces (`APPS_TS_TX_DATA`)
- **Use for custom tablespaces**
Performance Considerations

- **Impact is limited to CPU performance**
  - Data must be encrypted and decrypted
  - Highly dependent on access patterns to data

- **No disk I/O read or write impact**
  - Change is not significant

- **Column Encryption**
  - 5% to 20% CPU performance impact for several customers

- **Tablespace Encryption**
  - 10% to 15% CPU performance impact for one customer
Agenda

1. Sensitive Data Overview
2. Encryption
3. Controlling Data Access
4. Auditing
5. Q&A
# Oracle EBS Database Access Controls

## Defense in depth – implement layers!

| Application          | • Oracle EBS Application Security (roles/responsibilities/menus/functions)  
|                      | • Oracle EBS Personalizations  
|                      | • Application Data Masking (e.g., Mentis)  
| Database             | • Database Security (roles/privileges)  
|                      | • Fine Grained Access Controls (FGAC)  
|                      | • Oracle Database Vault  
| Operating System     | • Operating System Security  
|                      | • Sudo and Powerbroker  


Access to Sensitive Data

- **Block ad-hoc access to production database whenever possible**
  - **Integrigy #1 Security Recommendation**
  - Managed SQL*Net access
  - Oracle Connection Manager
  - Data center firewall – use VPN or jump servers

- **Database access is a key problem**
  - APPS_READ

- **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 Fine Grained Access Controls (FGAC)

- FGAC included with Oracle EBS database license

- FGAC policies allow blocking of access to column (returns null)
  - Modifies SQL at runtime to include a predicate clause for users included in policy

- Create policies by database role to block access to sensitive columns
  - Create roles so “default deny” – if role then allow
Oracle Database Vault with Oracle E-Business Suite
What is Database Vault?

- **Powerful protection**
  - Data protection realms
  - Control by IP address, time, etc.
  - Control SQL commands and other database operations

- **Provides segregation of duties between DBA and security administrator**

- **Add-on option licensed separately**
Database Vault and EBS Scenarios

- **Protect some DBAs from application data**
  - No protection for the SYSTEM, APPS, CTXSYS, or Oracle EBS module schema accounts
  - Named, non-application database accounts must be used for this level of protection – can be granted DBA role

- **Server/Database Consolidation**
  - Multiple applications running in Oracle E-Business Suite database (against best practice)
  - DBAs for other applications cannot access EBS data
<table>
<thead>
<tr>
<th>Realm Name</th>
<th>What is Protected</th>
<th>Who is authorized to access</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBS Realm</td>
<td>All tables in Oracle E-Business Suite Product Schemas</td>
<td>All Oracle E-Business Suite Product Schemas, and APPS, APPLSYS, SYSTEM, CTXSYS</td>
</tr>
<tr>
<td>EBS Realm - Applsys Schema</td>
<td>Most tables in the APPLSYS Schema</td>
<td>APPS, APPLSYS, SYSTEM, CTXSYS and APPS, APPLSYS, SYSTEM, CTXSYS</td>
</tr>
<tr>
<td>EBS Realm - Apps Schema</td>
<td>All objects in the APPS Schema (except the views)</td>
<td>APPS, APPLSYS, SYSTEM, CTXSYS and All product schemas, that uses intermedia indexes</td>
</tr>
<tr>
<td>EBS Realm - Applsyspub Schema</td>
<td>Objects required for EBS authorization</td>
<td>APPS, APPLSYS, SYSTEM, APPLSYS, CTXSYS and APPS, APPLSYS, SYSTEM, CTXSYS</td>
</tr>
<tr>
<td>EBS Realm - MSC Schema</td>
<td>Tables in the MSC Schema - except those that require partitions to be exchanged</td>
<td>APPS, APPLSYS, SYSTEM, CTXSYS and MSC</td>
</tr>
<tr>
<td>CTXSYS Data Dictionary</td>
<td>Objects in the CTXSYS Schema</td>
<td>All Oracle E-Business Suite 11i Product Schemas and APPS, APPLSYS, SYSTEM</td>
</tr>
</tbody>
</table>

Source: Oracle Metalink Note ID 428503.1
Agenda

1. Sensitive Data Overview
2. Controlling Data Access
3. Encryption
4. Auditing
5. Q&A
Auditing Access to Sensitive Data

- Native audit trail in Oracle Database and Oracle EBS can be accessed and manipulated by the DBA
  - SYSLOG auditing can be used to protect native database audit trail – DBA can disable it

- **External auditing solution required**
  - Protect audit trail in external database/appliance
  - Provide reporting and archiving of audit data
Data Scrambling/
Data Masking
Data Scrambling/Data Masking

- **Sensitive data in test & development must be scrambled**
  - Sensitive data inventory is critical to scrambling
  - Must periodically review database for instances of non-scrambled data as often in custom, interface, and temporary tables

- **Purge production as well as scramble**
  - Review data and transaction retention policy
  - Oracle EBS is “data in” for life – seldom purged
  - PCI Compliance = 1 to 2 years recommended retention
Data Scrambling/Data Masking

- **Data scrambling solutions**
  - Custom scripts – when just a few data elements
  - Oracle OEM Data Masking Pack (EBS Template)
  - Oracle AMP Data Masking (Cloning)
  - Mentis iScramble

- **Data Scrambling best practices**
  - Keep it simple – runtime and data issues
  - Use predictable data patterns to act as an ad-hoc control such as 7xx-xx-xxx for SSN
# How - Data Protection vs. Threats

## Data Access Method and Threats

<table>
<thead>
<tr>
<th>Data Access Method and Threats</th>
<th>1 - EBS Encrypt</th>
<th>2 - Trigger View</th>
<th>3 - Oracle TDE</th>
<th>4a - FGAC</th>
<th>4b - Internal Audit</th>
<th>4c - External Audit</th>
<th>3 + 4 - TDE + Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Application access by end-users (responsibility)</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>2. Application access by application administrators</td>
<td>E+</td>
<td>E-</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>3. Database access by DBA</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A+</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>4. Database access by Applications DBA (SYSTEM, APPS)</td>
<td>E+</td>
<td>E+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>5. Database access by other database accounts</td>
<td>E</td>
<td>E</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>6. Operating system access to database data files</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>7. On-line or off-line access to database backups</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>8. Exploitation of Oracle Applications security vulnerabilities</td>
<td>E-</td>
<td>E-</td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>9. Exploitation of Oracle Database security vulnerabilities</td>
<td>E+</td>
<td>E+</td>
<td>C+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
<td>A+</td>
</tr>
<tr>
<td>10. Exploitation of operating system security vulnerabilities</td>
<td>E</td>
<td>E</td>
<td>E</td>
<td></td>
<td></td>
<td>E</td>
<td></td>
</tr>
</tbody>
</table>

E = Encrypted,  C = Access Controlled,  A = Access Audited,  + = Mostly,  - = Partially
Agenda

1. Sensitive Data Overview
2. Controlling Data Access
3. Encryption
4. Auditing
5. Q&A
Contact Information

Stephen Kost  
Chief Technology Officer  
Integrigy Corporation

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