Oracle EBS Sensitive Administrative Pages Are You Overlooking This Threat?

April 24, 2013

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

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Speakers

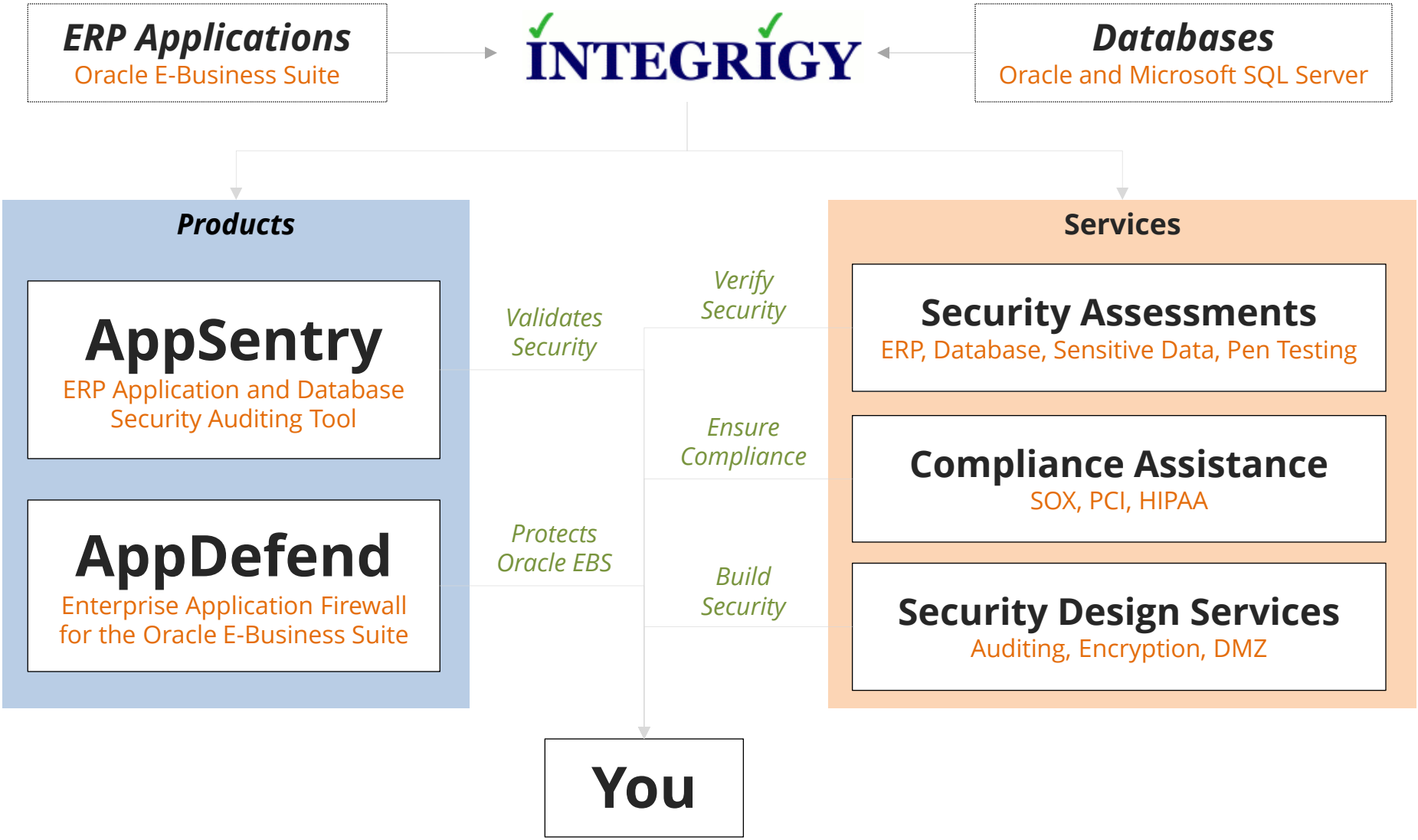
Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- Founder of ERP Risk Advisors 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



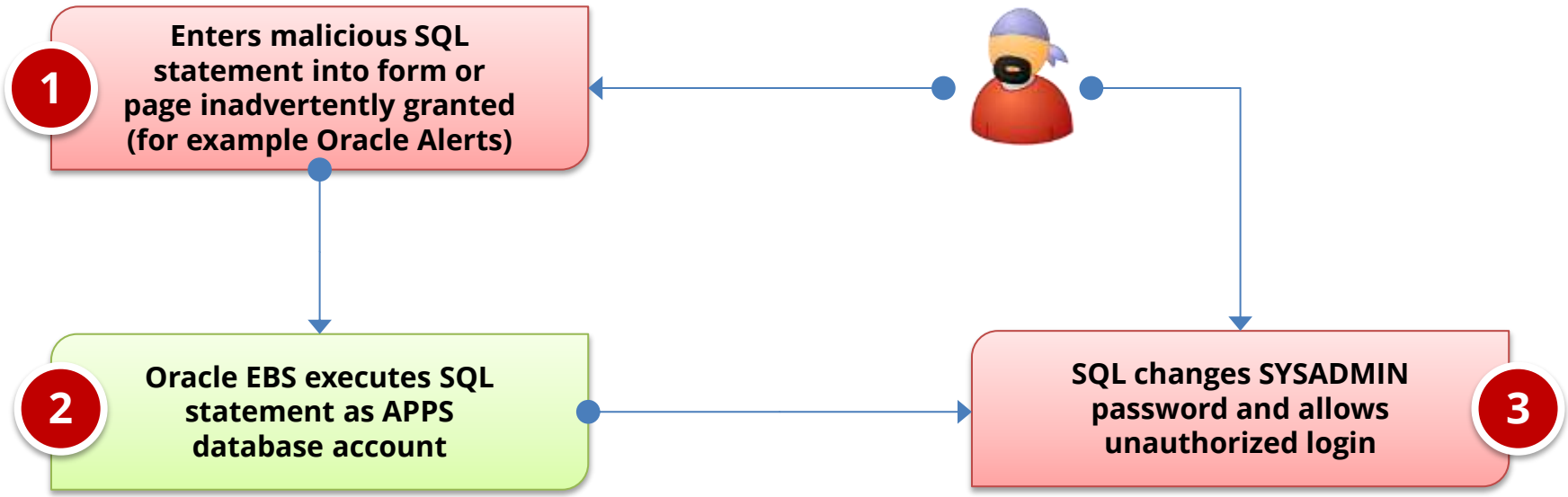
Sensitive Administrative Pages

MOS 1334930.1 *Sensitive Administrative Pages in Oracle E-Business Suite*

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.

Threat

Non-privileged users may be able to execute SQL as the APPS database account or operating system commands as the database owner.



Sensitive Administrative Pages Risks

- **Execution of SQL statements (DDL/DML/functions) that may be used to circumvent application controls**
  All SQL executed as APPS database account

- **Fraud or data theft by non-privileged users due to lack of controls over sensitive administrative pages**
  Are these pages and functions in your SOD matrix?

- **Bypassing of auditing and applications controls by privileged applications users**
  Second-order attack – indirectly occurs later when SQL executed

Sensitive Administrative Page Access

Access to sensitive administrative pages may be controlled by multiple security mechanisms within Oracle EBS.

- **Forms**
  Professional interface forms controlled by menus, functions, and grants
- **HTML Pages**
  HTML web pages controlled by menus, functions, and grants
- **Features via Profile Options**
  Core EBS features like “Examine” controlled by system profile options
- **JTF Permissions and Roles**
  CRM functionality may be controlled by JTF permissions and roles

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
- 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

HTML Pages that Allow SQL **(Partial Listing)**

- AME Admin Dashboard
- AME Business Analyst Dashboard
- Create Parameterized Query Template
- Create page for Profiles
- Search page for Profiles
- Update page for Profiles
- Define page for Profile Values
- Function Search
- SSWA Maintain Objects
- Object Details
- IBU_A_PZ_FN
- IBU_A_UG_FN
- IEU_PROVIDER_SITE
- JTF_FM_ALLQUERY
- JTF_FM_VIEWDOCS
- OAM Create Test
- Maintain SCORM Adapter Properties
- Maintain Learning Object Properties

Show query of ALR_ALERTS

Demonstrate Oracle Alerts and change SYSADMIN password

Profile Options

Oracle EBS Feature	Profile Option Name	Recommended Setting
OA Framework Personalization	Personalize Self-service Defn (FND_CUSTOM_OA_DEFINTION)	No
Form Personalization	**Combination of profiles options** Hide Diagnostics menu entry (FND_HIDE_DIAGNOSTICS) Utilities:Diagnostics (DIAGNOSTICS)	Hide: Yes Utilities:Diagnostics: No
Examine	**Combination of profiles options** Hide Diagnostics menu entry (FND_HIDE_DIAGNOSTICS) Utilities:Diagnostics (DIAGNOSTICS)	Hide: Yes Utilities:Diagnostics: No

Demonstrate Examine Feature

Show Profile Options Query

JTF Permissions and Roles

CRM Feature	Profile Option Name
CRM Declarative Component Framework	**JTF_ADMIN_PERM** Permission (part of the JTF_SYSTEM_ADMIN_ROLE)
Email Center	**The JTF_FM_ADMIN** (Fulfillment Administrator) role provides access to the Query tab in the Oracle Email Center administration console.
Knowledge: Authoring	CS_Assoc_Ext_Obj_To_Sol permission controls ability to attach external objects to a solution in Oracle Knowledge Management

Sensitive Administrative Pages (Forms/HTML)

- **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

Show Oracle SQL Queries

Show Oracle SQL Queries Output

Sensitive Administrative Pages (Forms/HTML)

- **All changes to these forms should go through change management process**
  Audit or sample changes and review SQL statements

- **Require DBA or peer review of all SQL statements for both security and performance reasons**
  IT Security and Auditors generally not qualified to identify issues

- **Audit access to forms/pages and table activity, especially SQL statements**
  Sample access and table changes to review for appropriateness

Sensitive Administrative Pages (Profile Options)

- **System profile options should be part of the change management process**
  Audit or sample changes and review SQL statements

- **Audit all changes to system profile option value changes**
  May need to use database auditing rather than EBS audit trails

- **Review system profile options at all levels**
  Values may be set to site, application, responsibility, or user level

Upcoming Webinar

Oracle EBS Account Password Decryption Threat Explored

Thursday, May 23rd, 2013

2:00m EDT

www.integrigy.com/upcoming-events

Resources

Integrigy's Website	www.integrigy.com Oracle EBS Security Whitepapers and Blog	
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 E-Business Suite Controls: Application Security Best Practices* [Amazon]	
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:
- http://www.erpra.net/WebinarAccessPage.html
- 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**
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**
youtube: **youtube.com/integrigy**