ERP Risk Advisors

INTEGRIGY

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

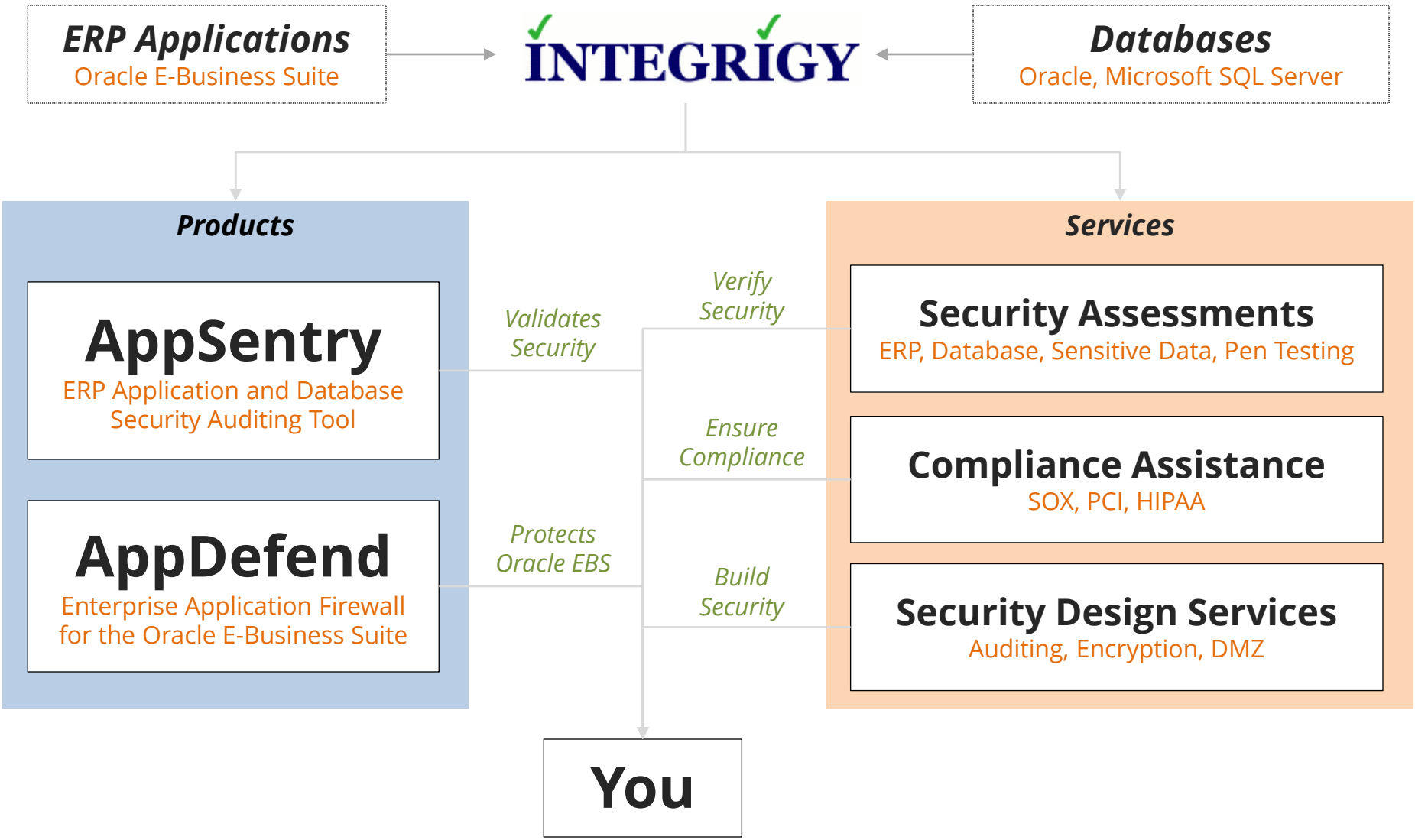
Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- 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*

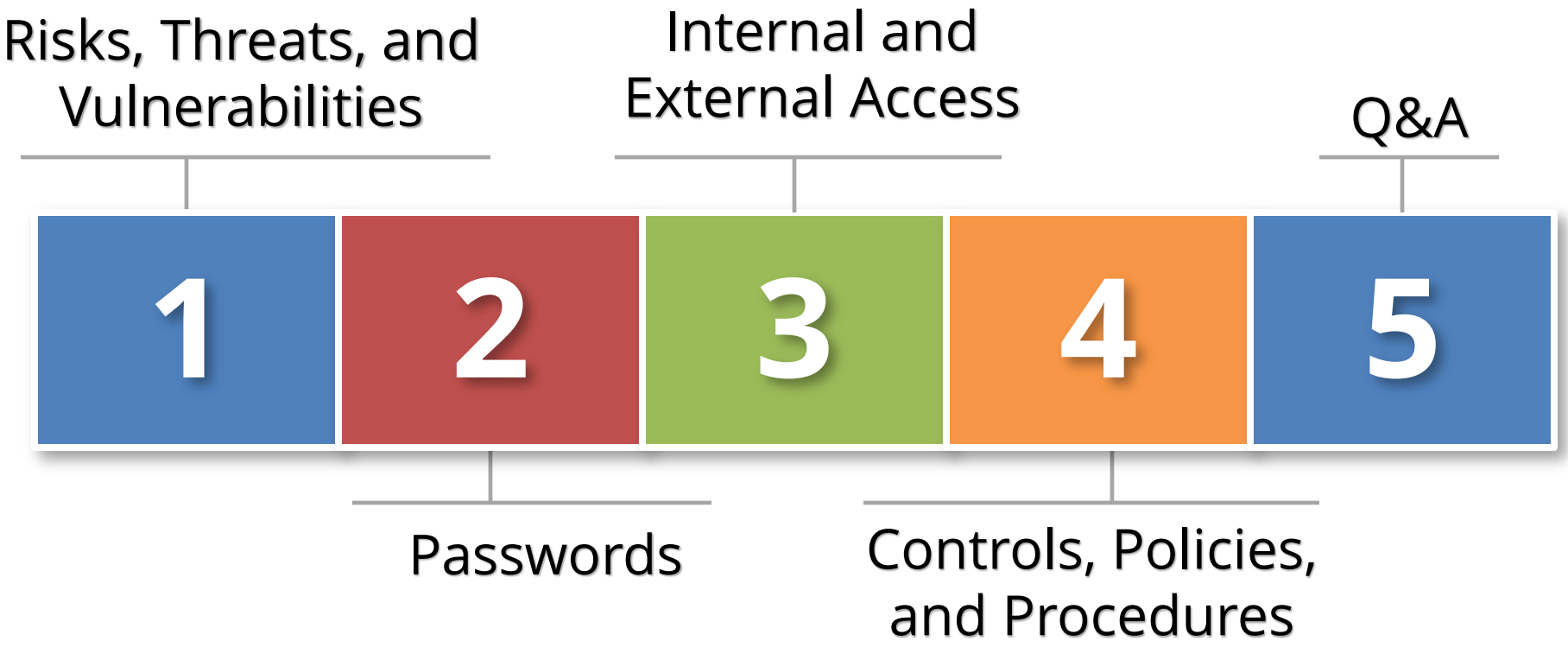
Stephen Kost
Integrigy Corporation

- 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



Agenda


Risks, Threats, and Vulnerabilities
Internal and External Access
Q&A
1
2
3
4
5
Passwords
Controls, Policies, and Procedures

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

Risks and Threats ▪ examples	**1** DB Pass	**2** App Pass	**3** Direct Access	**4** App Sec Design	**5** Extern App	**6** Patch Policy	**7** SQL Forms	**8** Change Control	**9** Audit	**10** Pass Control
1. Sensitive data loss (data theft) ▪ Bulk download via direct access ▪ Bulk download via indirect access										
2. Direct entering of transactions (fraud) ▪ Update a bank account number ▪ Change an application password										
3. Misuse of application privileges (fraud) ▪ Bypass intended app controls ▪ Access another user's privileges										
4. Impact availability of the application ▪ Wipe out the database ▪ Denial of service (DoS)										

1 Default Database Passwords

- Oracle E-Business Suite database is delivered with up to **300 database accounts**
  - Default passwords (GL = GL)
  - Active
  - **Significant privileges**

Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* 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

2 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

Active Application Account	Default Password	Active Responsibilities
ASGADM	WELCOME	▪ SYSTEM_ADMINISTRATOR ▪ ADG_MOBILE_DEVELOPER
IBE_ADMIN	WELCOME	▪ IBE_ADMINISTRATOR
MOBADM	MOBADM	▪ MOBILE_ADMIN ▪ SYSTEM_ADMINISTRATOR
MOBILEADM	WELCOME	▪ ASG_MOBILE_ADMINISTRAOTR ▪ SYSTEM_ADMINISTRATOR
OP_CUST_CARE_ADMIN	OP_CUST_CARE_ADMIN	▪ 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

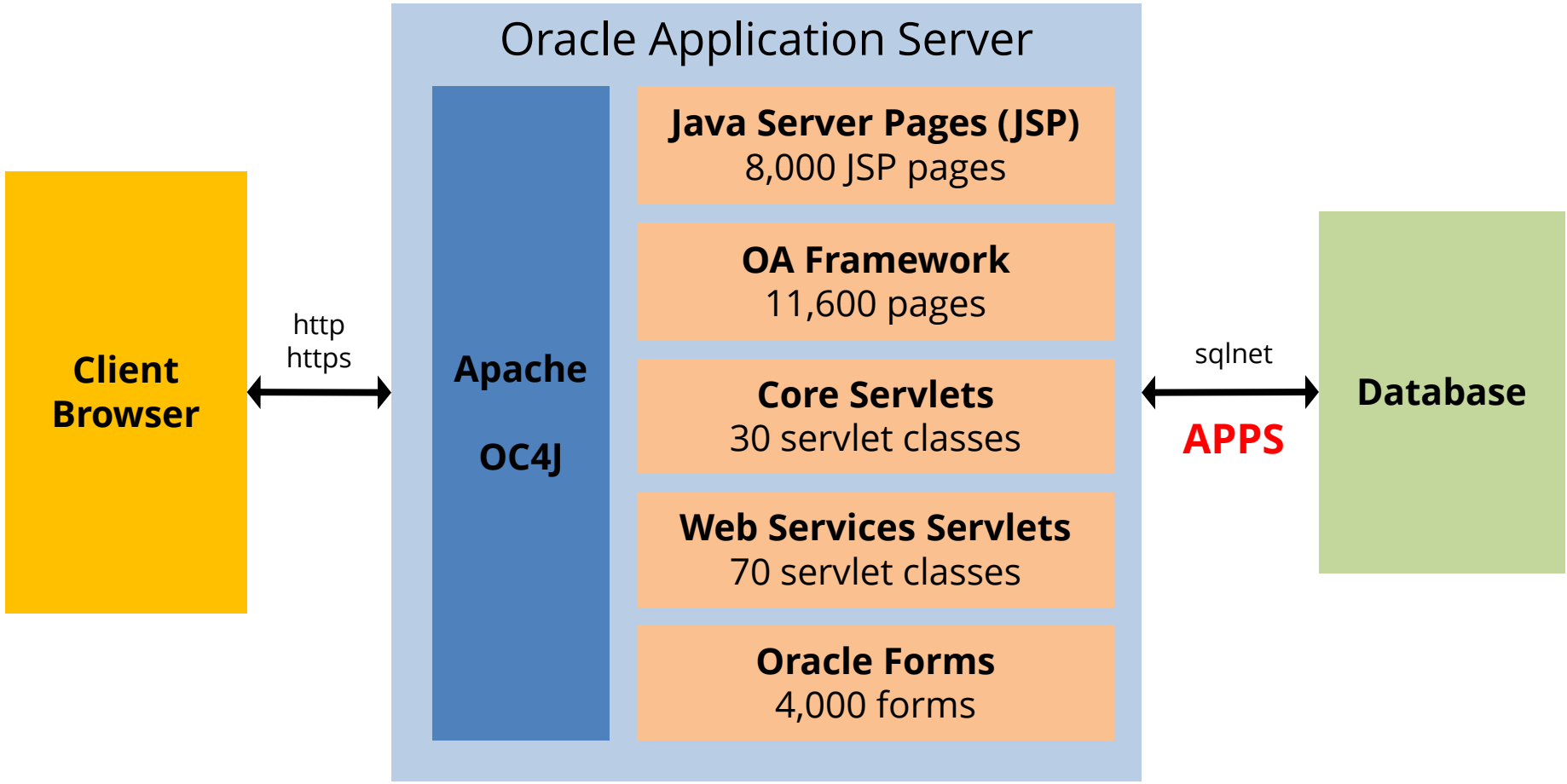
3 Direct Database Access

- 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

5 External Access Configuration



- 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)

Oracle EBS DMZ Oracle Support Notes

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
4. Configuration Review - Manual
   - Review 8 major configuration steps
5. Configuration Review - AppSentry
   - Automates checking 6 of 8 major configuration steps

7 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

Weak Application Password Controls

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

System Profile Options	***11i Default***	***R12 Default***
Signon Password Failure Limit	(null)	10
Signon Password Hard To Guess (1 letter, 1 number, no repeating characters, not username)	No	No
Signon Password Length	5	6
Signon Password No Reuse	(null)	(null)
Signon Password Case	insensitive	insensitive

Signon Password settings must be changed to meet organization's password policy

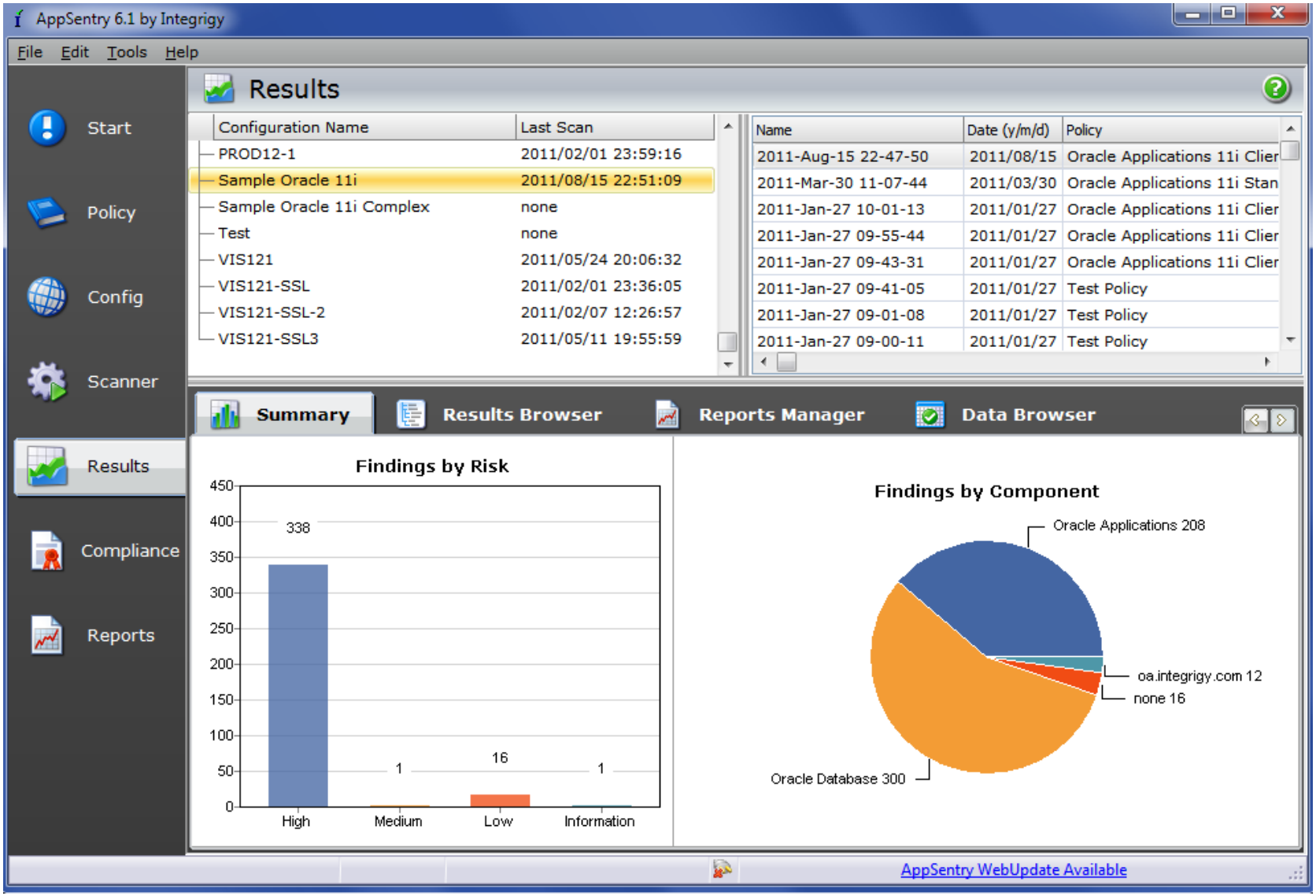
Oracle EBS Password Decryption

- 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

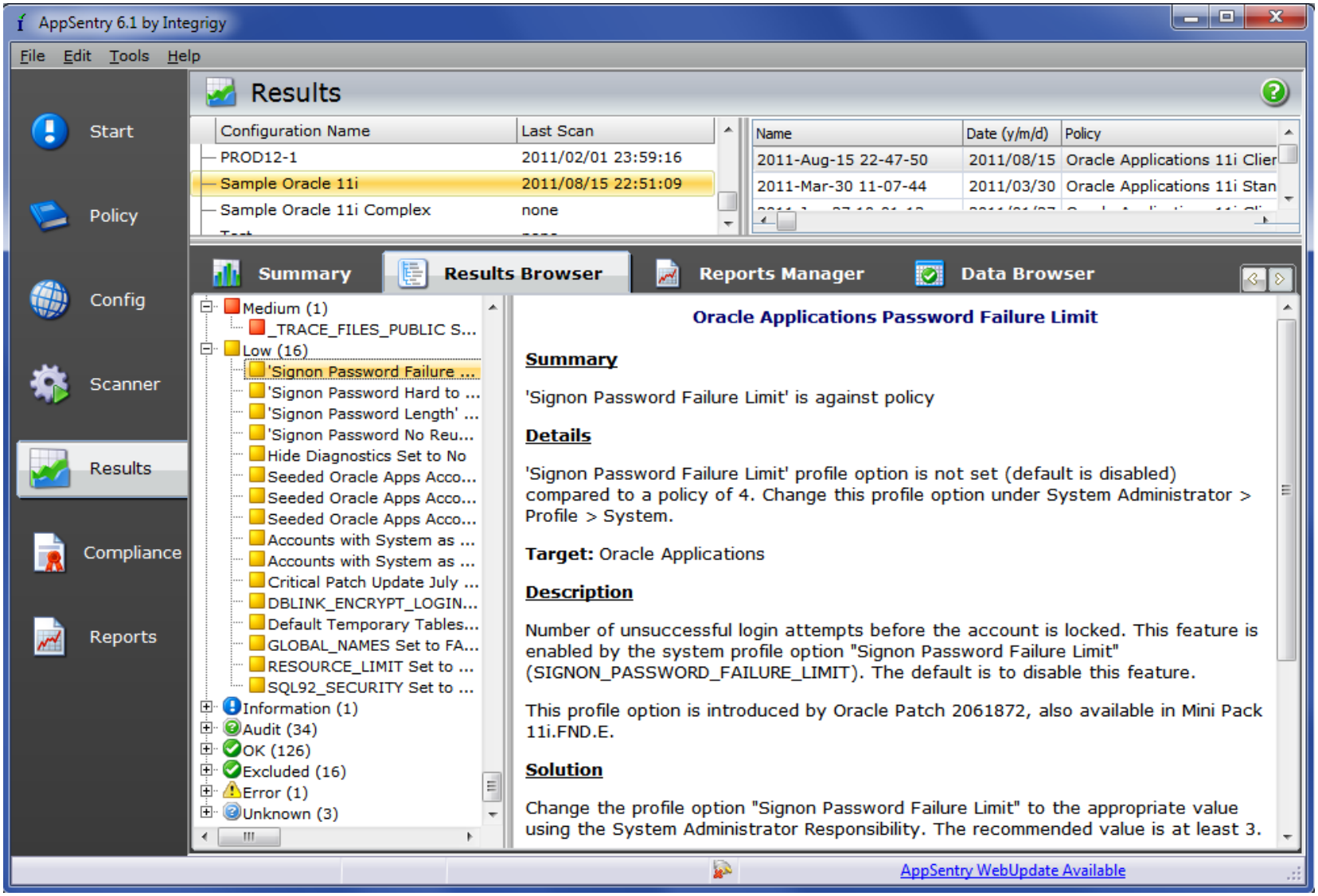
How to Check Password Controls

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


AppSentry 6.1 by Integrigy
File Edit Tools Help
Start
Policy
Config
Scanner
Results
Compliance
Reports
Results
Configuration Name
Last Scan
PROD12-1
2011/02/01 23:59:16
Sample Oracle 11i
2011/08/15 22:51:09
Sample Oracle 11i Complex
none
Test
none
VIS121
2011/05/24 20:06:32
VIS121-SSL
2011/02/01 23:36:05
VIS121-SSL-2
2011/02/07 12:26:57
VIS121-SSL3
2011/05/11 19:55:59
Name
Date (y/m/d)
Policy
2011-Aug-15 22-47-50
2011/08/15
Oracle Applications 11i Clier
2011-Mar-30 11-07-44
2011/03/30
Oracle Applications 11i Stan
2011-Jan-27 10-01-13
2011/01/27
Oracle Applications 11i Clier
2011-Jan-27 09-55-44
2011/01/27
Oracle Applications 11i Clier
2011-Jan-27 09-43-31
2011/01/27
Oracle Applications 11i Clier
2011-Jan-27 09-41-05
2011/01/27
Test Policy
2011-Jan-27 09-01-08
2011/01/27
Test Policy
2011-Jan-27 09-00-11
2011/01/27
Test Policy
Summary
Results Browser
Reports Manager
Data Browser
Findings by Risk
450
400
350
300
250
200
150
100
50
0
338
1
16
1
High
Medium
Low
Information
Findings by Component
Oracle Applications 208
oa.integrigy.com 12
none 16
Oracle Database 300
AppSentry WebUpdate Available

AppSentry


AppSentry 6.1 by Integrigy
File Edit Tools Help
Start
Policy
Config
Scanner
Results
Compliance
Reports
Results
Configuration Name
Last Scan
PROD12-1
2011/02/01 23:59:16
Sample Oracle 11i
2011/08/15 22:51:09
Sample Oracle 11i Complex
none
Name
Date (y/m/d)
Policy
2011-Aug-15 22-47-50
2011/08/15
Oracle Applications 11i Clier
2011-Mar-30 11-07-44
2011/03/30
Oracle Applications 11i Stan
Summary
Results Browser
Reports Manager
Data Browser
Medium (1)
_TRACE_FILES_PUBLIC S...
Low (16)
'Signon Password Failure ...
'Signon Password Hard to ...
'Signon Password Length' ...
'Signon Password No Reu...
Hide Diagnostics Set to No
Seeded Oracle Apps Acco...
Seeded Oracle Apps Acco...
Seeded Oracle Apps Acco...
Accounts with System as ...
Accounts with System as ...
Critical Patch Update July ...
DBLINK_ENCRYPT_LOGIN...
Default Temporary Tables...
GLOBAL_NAMES Set to FA...
RESOURCE_LIMIT Set to ...
SQL92_SECURITY Set to ...
Information (1)
Audit (34)
OK (126)
Excluded (16)
Error (1)
Unknown (3)
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.
AppSentry WebUpdate Available

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 E-Business Suite Controls: Application Security Best Practices*
- 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**