ERP Risk Advisors

INTEGRIGY

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

Speakers

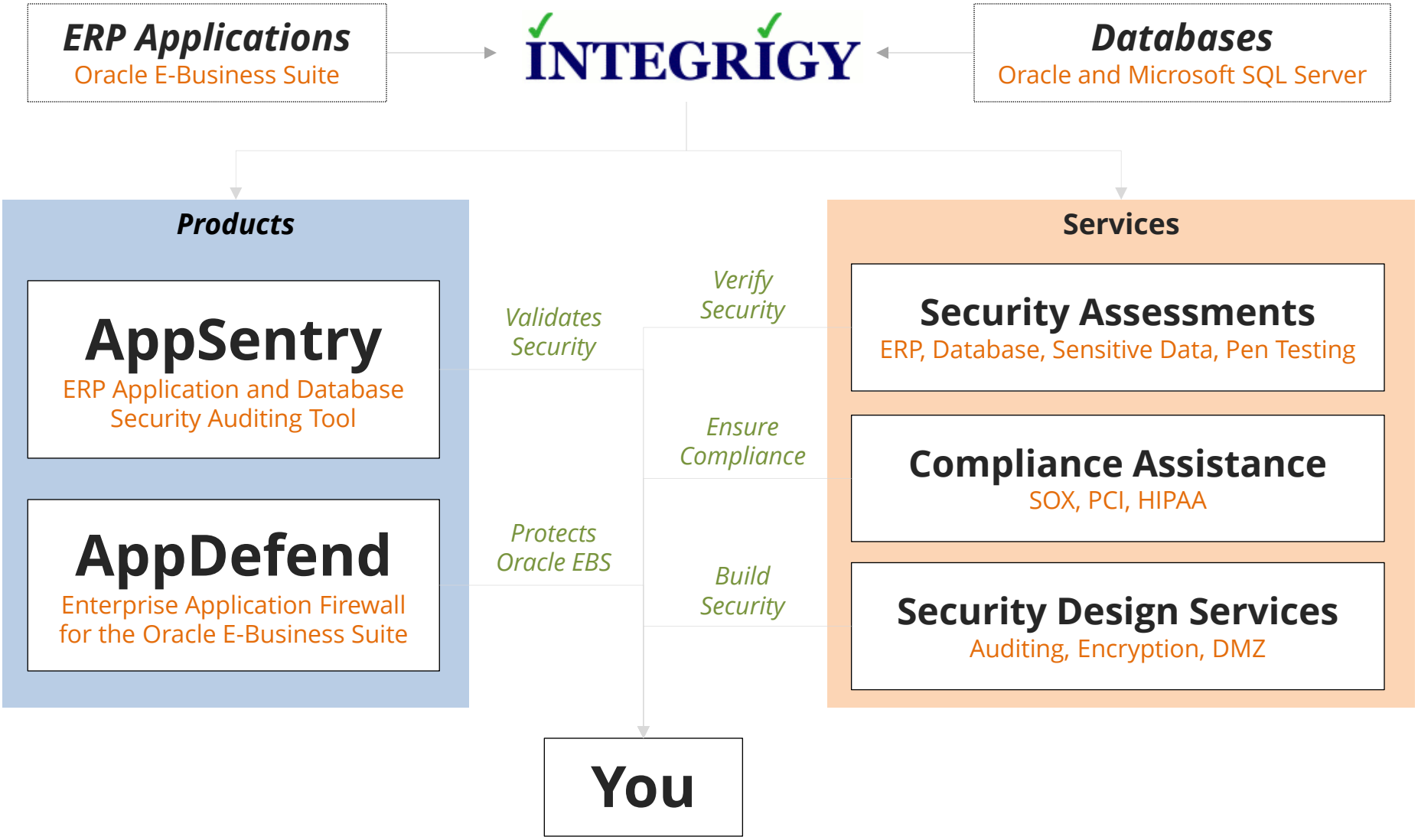
Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- 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*

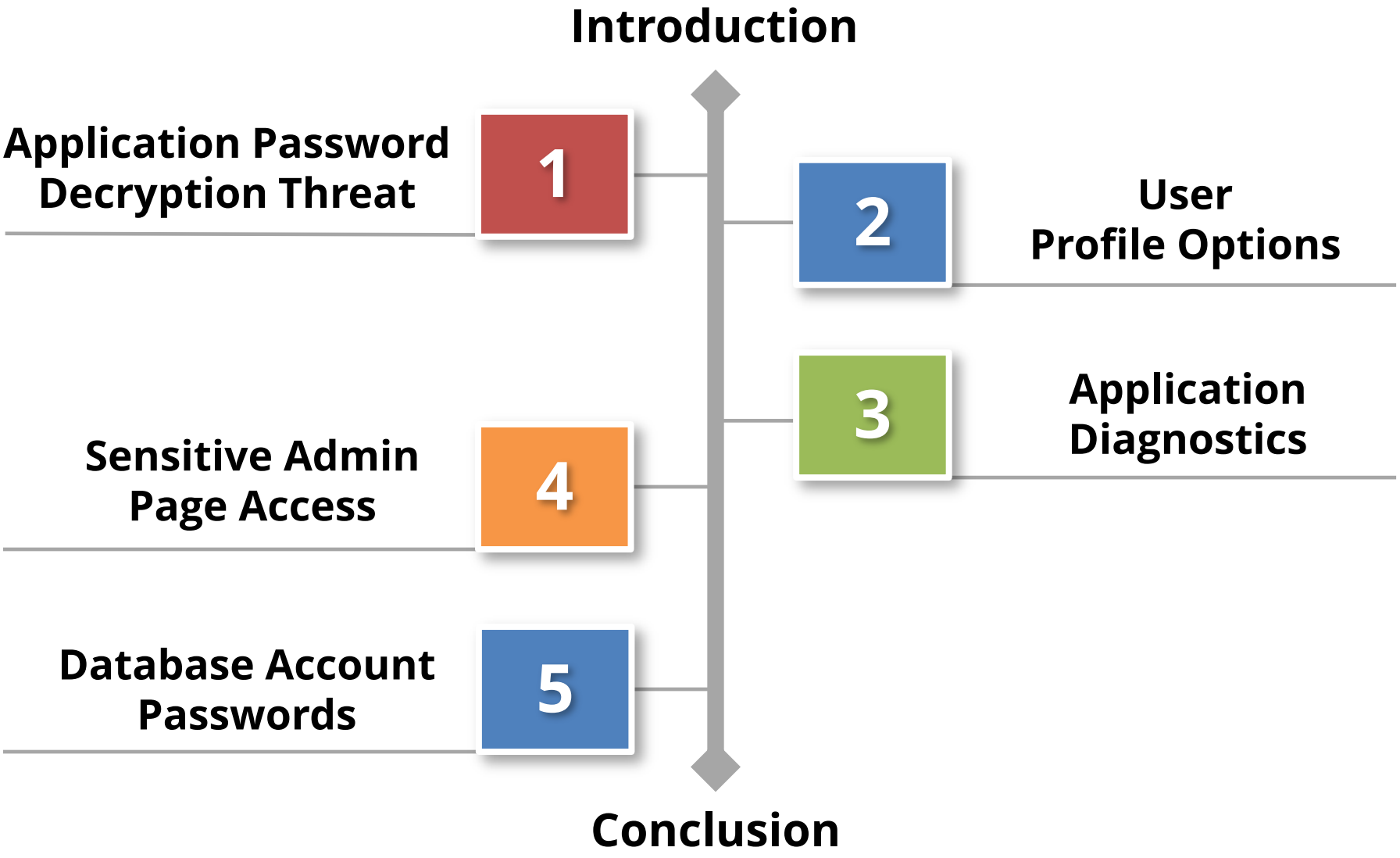
Stephen Kost
Integrigy Corporation

- 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



Agenda


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

Agenda

Introduction

1 Application Password Decryption Threat

2 User Profile Options

3 Application Diagnostics

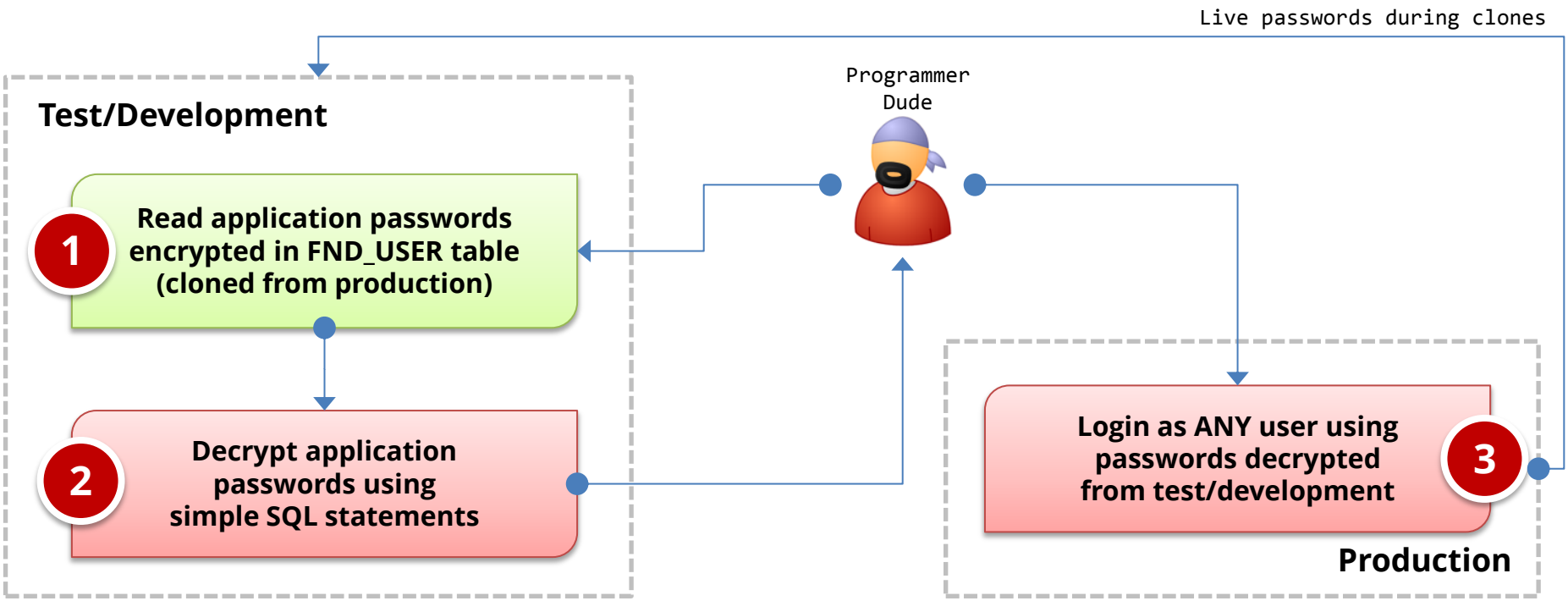
4 Sensitive Admin Page Access

5 Database Account Passwords

Conclusion

Threat

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



Oracle EBS Password Encryption

FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	ZG6EBD472D1208B0CDC78D7EC7730F9B249496F825E761BA3EB2FEBB54F6915FADA757EF4558CF438CF55D23FE32BE0BE52E	ZG6C08D49D524A1551A3068977328B1AFD260400FB598E799A3A8BAE573777E7EE7262D1730366E6709524C95EC6BFA0DA06
SYSADMIN	ZH39A396EDCA4CA7C8D5395D94D8C915510C0C90DA198EC9CDA15879E8B547B9CDA034575D289590968F1B6B38A1E654DD98	ZHF57EAF37B1936C56755B134DE7C83AE40CADDD4AA83B1D7455E5533DC041773B494D2AA04644FB5A514E5C5614F3C87888
WIZARD	ZG2744DCFCCFFA381B994D2C3F7ADACF68DF433BADF59CF6C3DAB3C35A11AAAB2674C2189DCA040C4C81D2CE41C2BB82BFC6	ZGE9AAA974FB46BC76674510456C739564546F2A0154DCF9EBF2AA49FBF58C759283C7E288CC673044036E284042A8FE4451

APPS password encrypted user name + user password

User password encrypted using APPS password

Password Decryption SQL – 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))
```

Google: oracle applications password decryption

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

Introduction

1 Application Password Decryption Threat

2 **User Profile Options**

3 Application Diagnostics

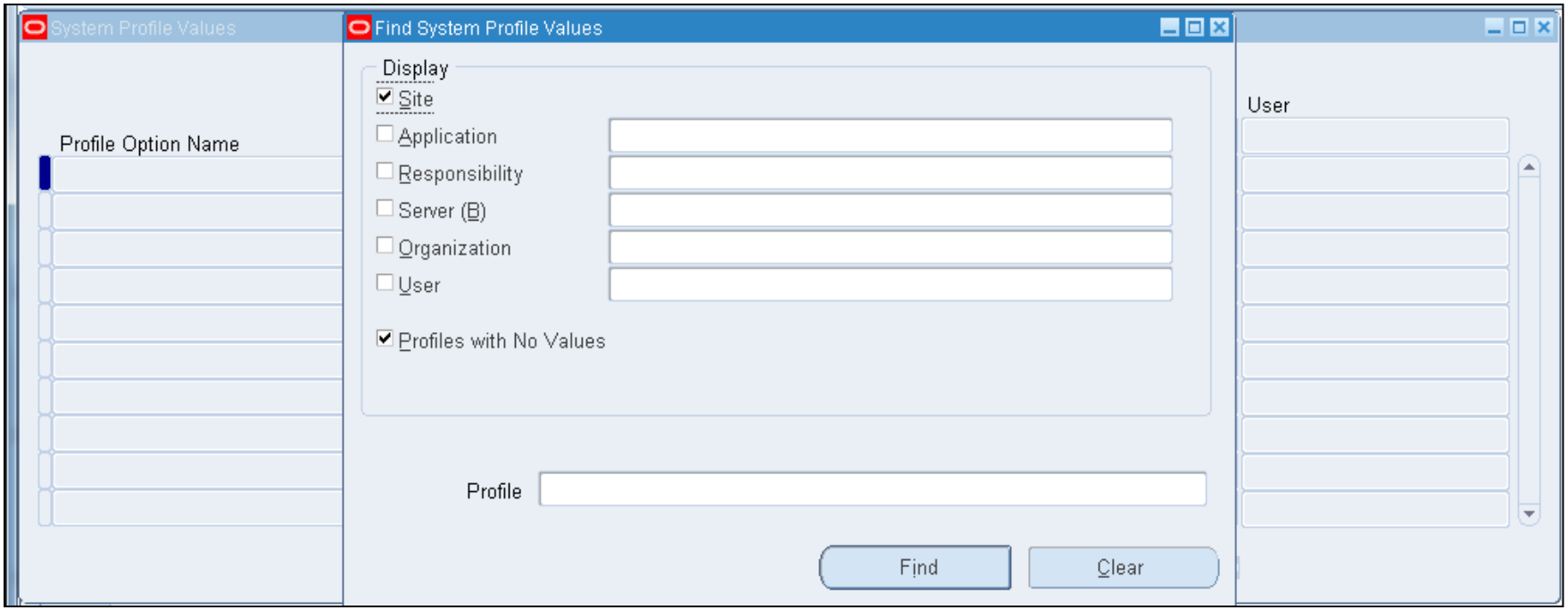
4 Sensitive Admin Page Access

5 Database Account Passwords

Conclusion

User Profile Values

- Profile Options can be set through the System Profile Values form:



User Profile Values

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

Personal Profile Values

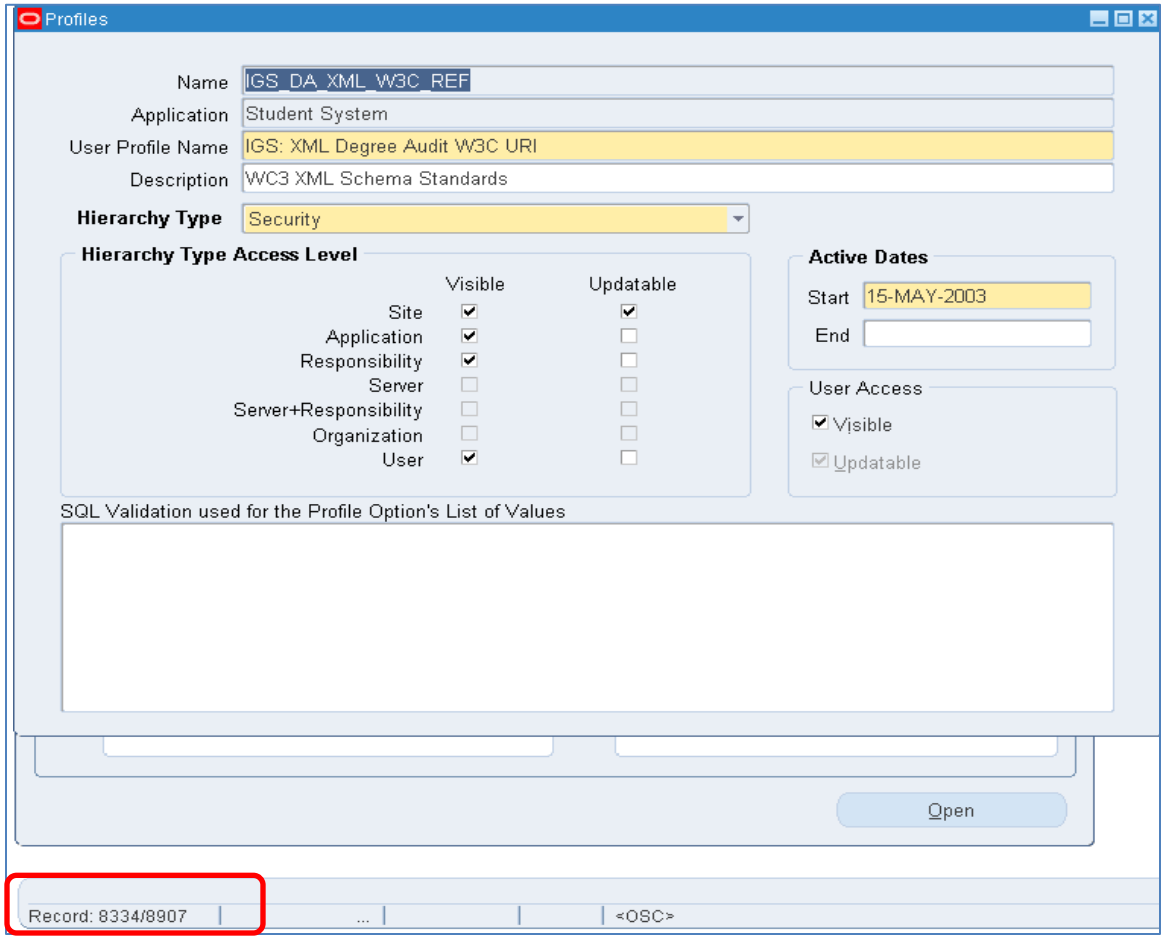
Profile Name	Default Value	User Value
%WSH%		
@JL : Perform Inflation Adjustmer		
ABM: ABM Analyzer Help	/OA_DOC/abmaug1110.pdf	
ABM: ABM Help	/OA_DOC/abmug1110.pdf	
ABM: Dark Color RGB String		
ABM: Java Currency Format String	##,###,###,##0.00000	
ABM: Java Date Format String	dd-MMM-yyyy	
ABM: Java Date-Time Format Strir	dd-MMM-yyyy hh:mm:ss	
ABM: Java Numeric Format String	##,###,###,##0.######	
ABM: Light Color RGB String		
ABM: Look And Feel Class		
ABM: Medium Color RGB String		

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:

Profiles

Name: GL_JRNL_REVW_REQUIRED
Application: General Ledger
User Profile Name: GL: Journal Review Required
Description: Journal review required before posting
Hierarchy Type: Security

Hierarchy Type Access Level

	Visible	Updatable
Site	☑	☑
Application	☑	☑
Responsibility	☑	☑
Server	☐	☐
Server+Responsibility	☐	☐
Organization	☐	☐
User	☑	☑

Active Dates
Start: 01-JAN-1951
End:

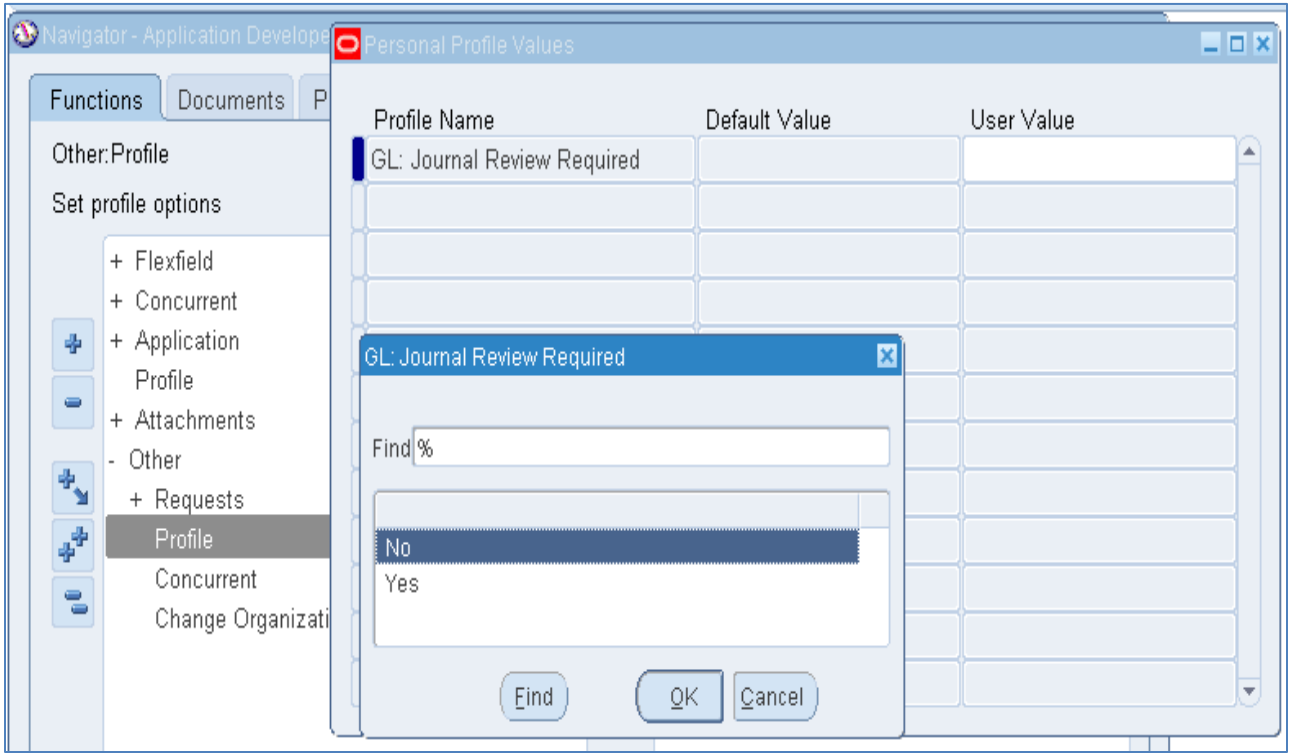
User Access
☑ Visible
☑ Updatable

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

```
SQL="SELECT MEANING \"Jrnl review required\",
LOOKUP_CODE
INTO :visible_option_value,
:profile_option_value
FROM fnd_lookups
WHERE lookup_type = 'YES_NO'"
COLUMN="\"Jrnl review required\"(30)"
```

User Profile Values

- Example:



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

Agenda

Introduction

1 Application Password Decryption Threat

2 User Profile Options

3 **Application Diagnostics**

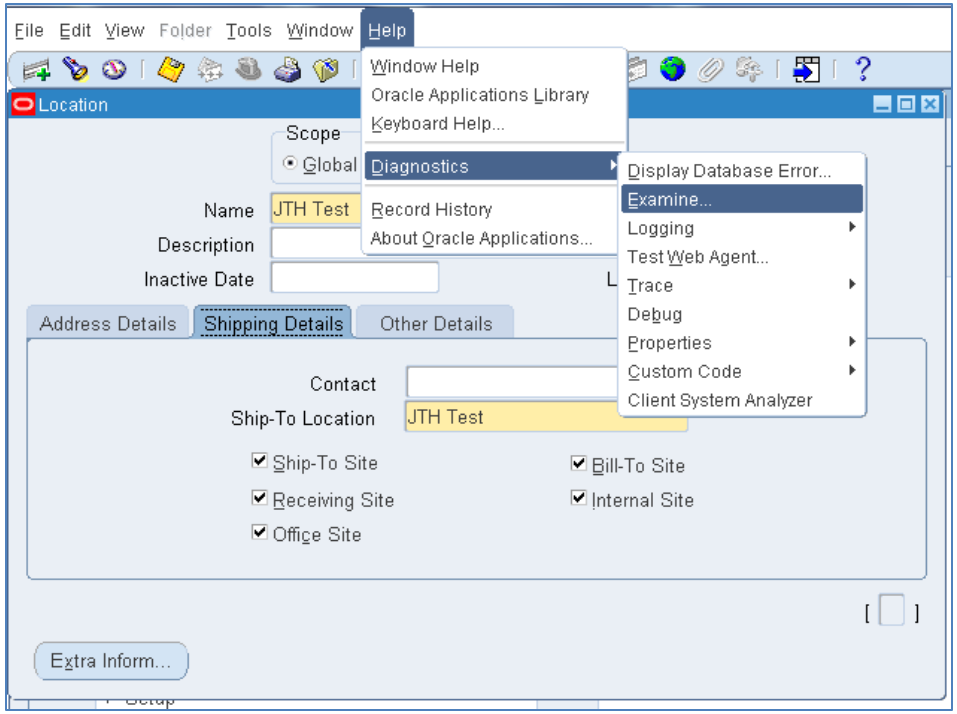
4 Sensitive Admin Page Access

5 Direct Database Account Access

Conclusion

Application Diagnostics

- Represents ‘back door’ access to tables
- Enabled through Utilities: Diagnostics profile option

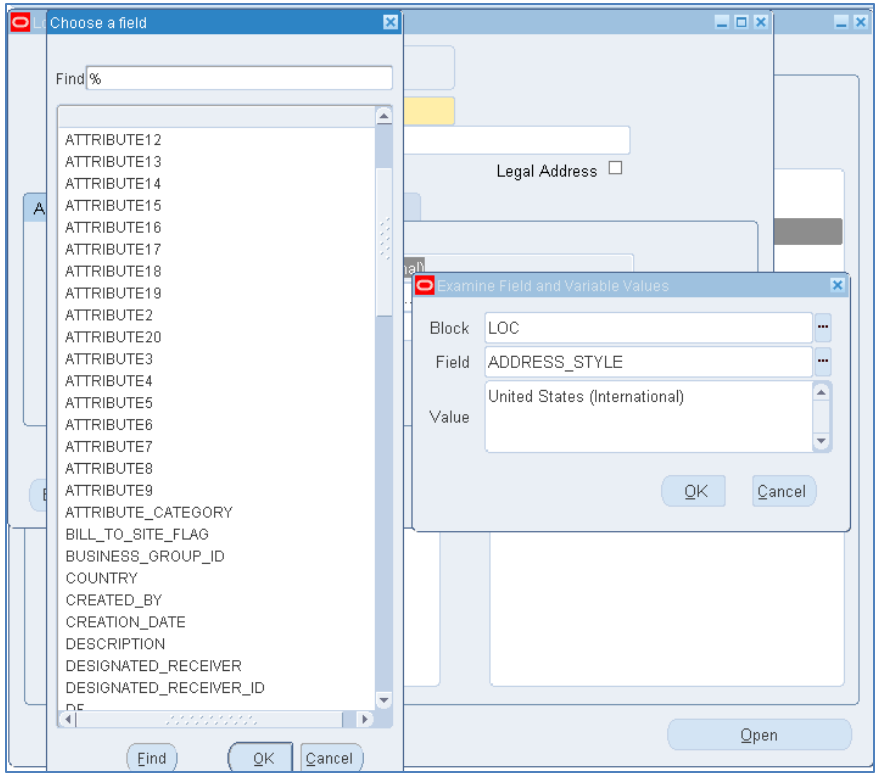


Application Diagnostics

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

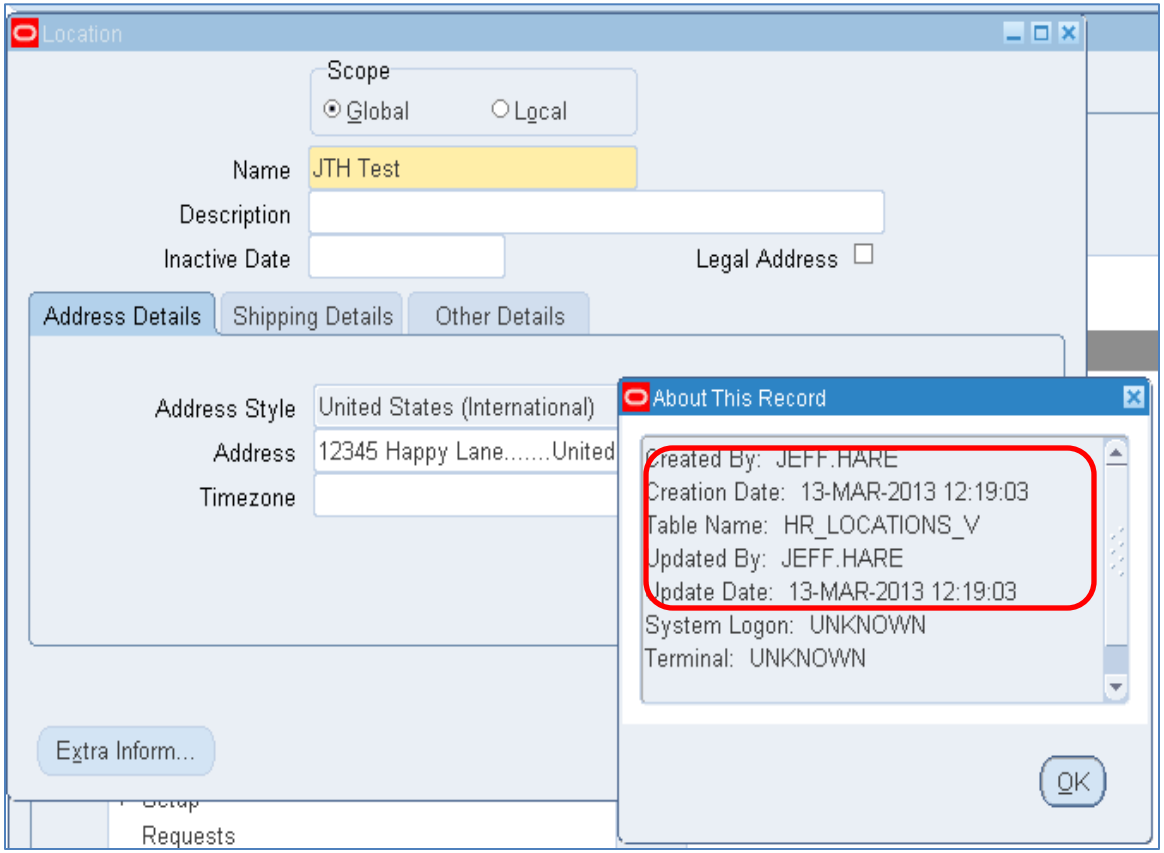
Application Diagnostics

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



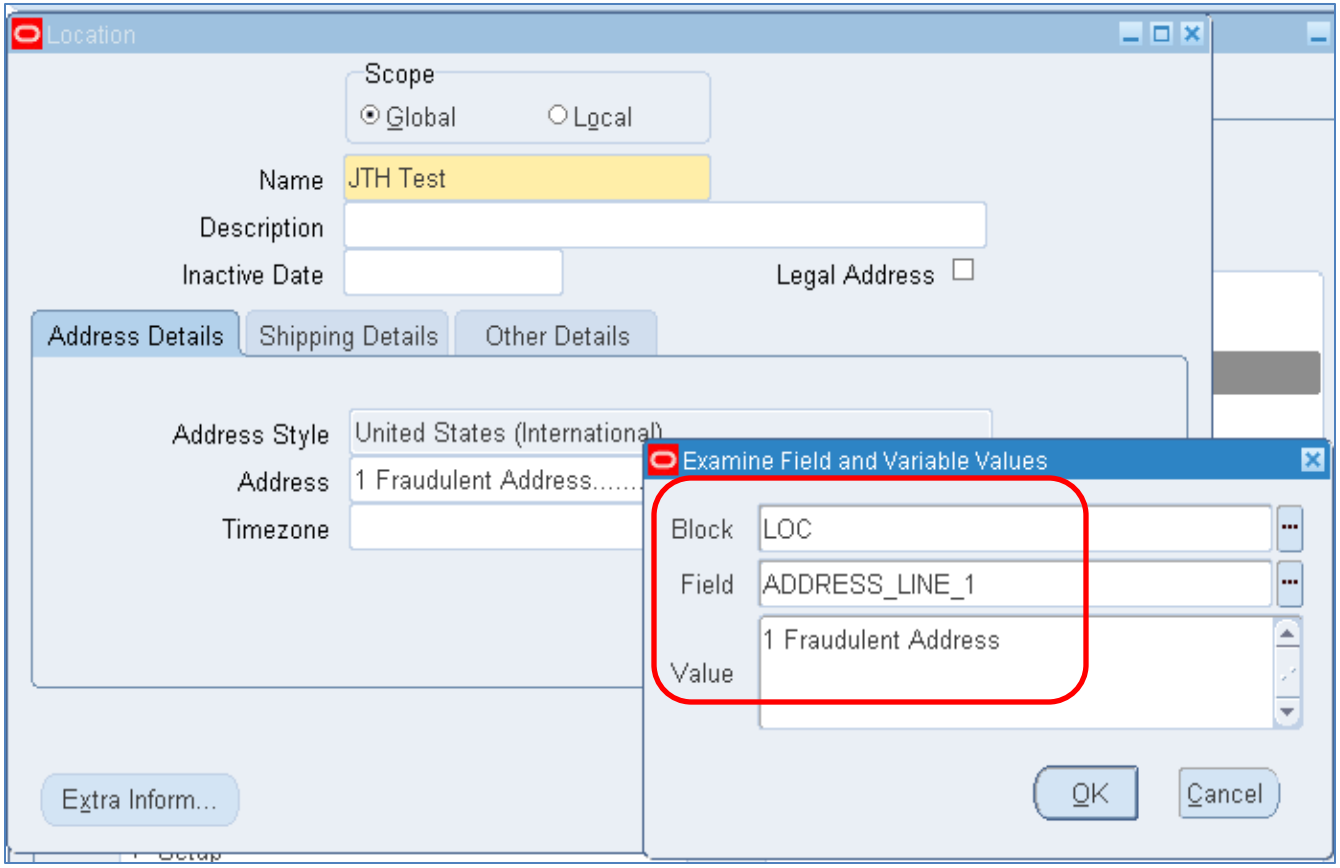
Application Diagnostics

- Example – before:



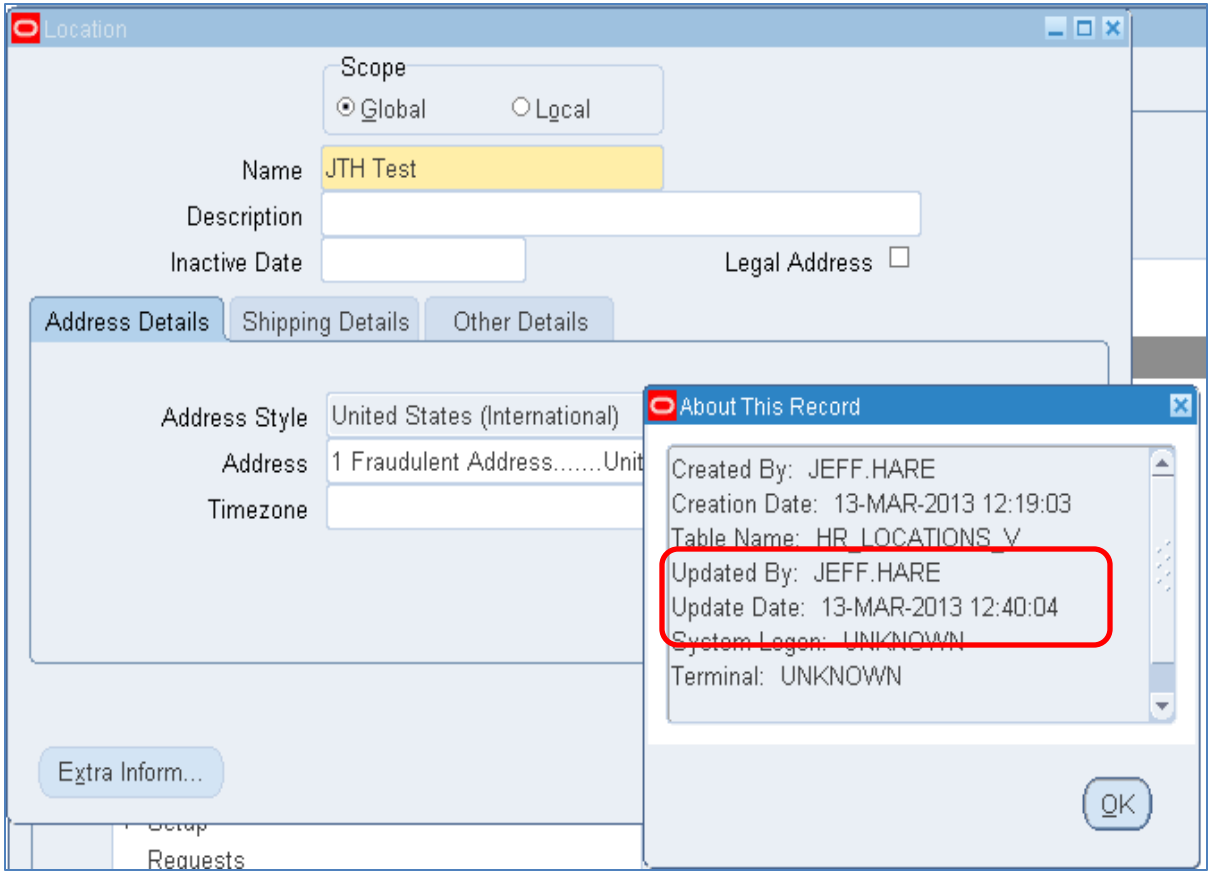
Application Diagnostics

- 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

Agenda

Introduction

1 Application Password Decryption Threat

2 User Profile Options

3 Application Diagnostics

4 **Sensitive Admin Page Access**

5 Database Account Passwords

Conclusion

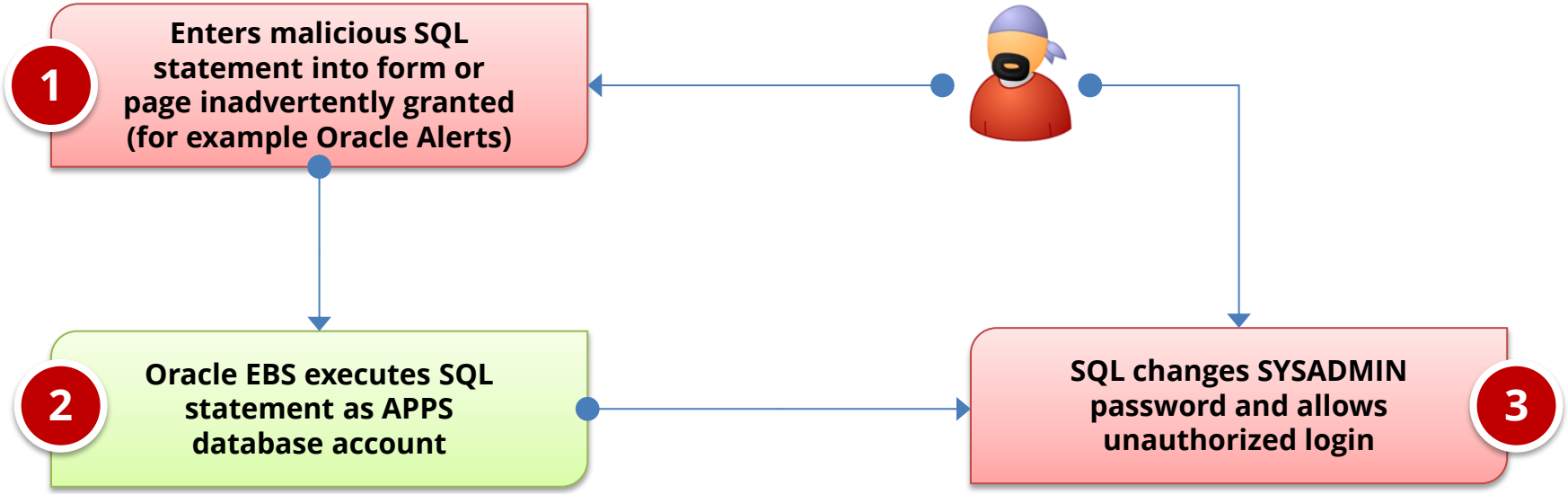
Sensitive Administrative Pages

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.



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

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 priviliege 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

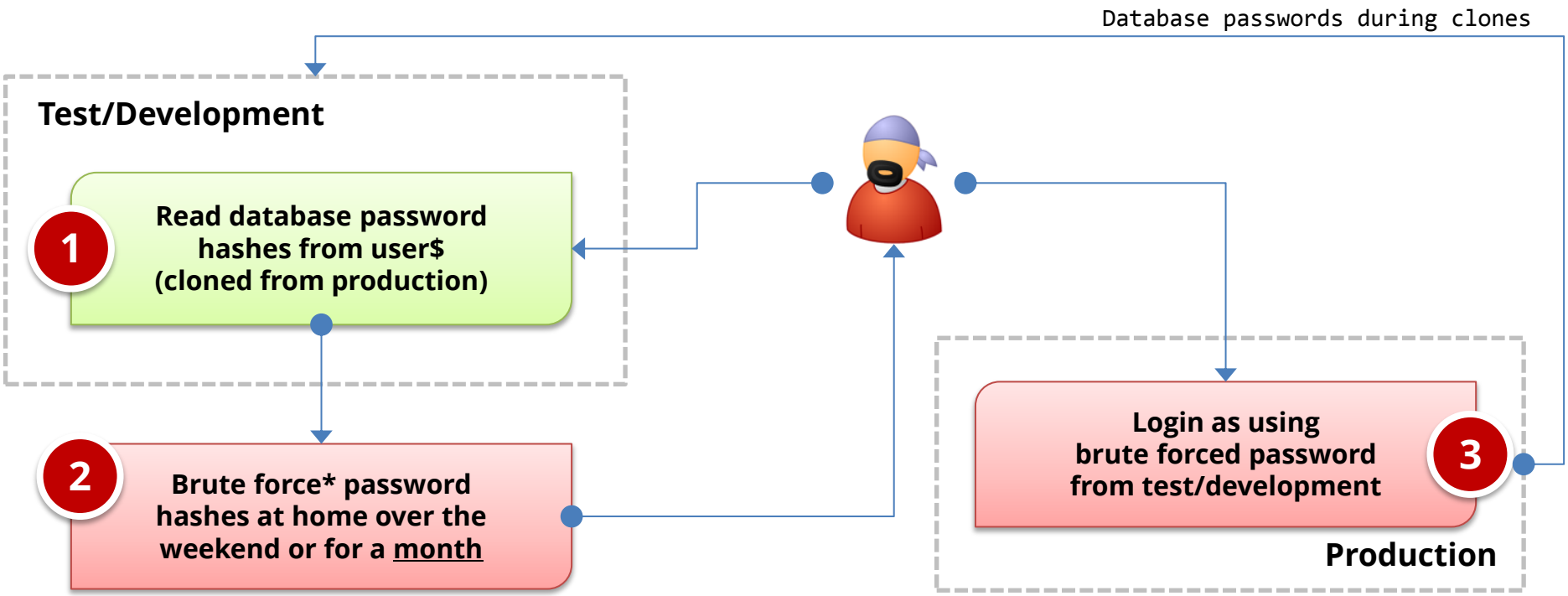
4 Sensitive Admin Page Access

5 **Database Account Passwords**

Conclusion

Threat

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



*Google: oracle password cracker

Database Password Facts

- 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

EBS Database Account Facts

- 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

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

Brute Forcing Database Passwords

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 –

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

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

Agenda

Introduction

1 Application Password Decryption Threat

2 User Profile Options

3 Application Diagnostics

4 Sensitive Admin Page Access

5 Database Account Passwords

>>> Conclusion <<<

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.integrigy.com/upcoming-events
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**