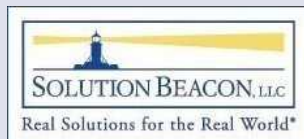


Better R11i Security In 3 Days Keeping the Bad Guys Away (Part II)

Randy Giefer
Solution Beacon, LLC



Today's Agenda:

- Presenter Introductions
- Presentation Overview
- 30 Minute Release 11i Security
- Minute 31 and Beyond – Your Next Steps For The Next 3 Days
- Questions and Answers

Presenter – Randy Giefer

- 20+ years of IT experience
 - Databases and Applications
 - 10 years Oracle Apps DBA
 - Fortune 1-1000
 - Government
- Founder of Solution Beacon, LLC
- Security Practice
- Email: rgiefer@solutionbeacon.com

Presentation Overview

- 1/2 Awareness
- 1/2 Real World Best Practices
- Follow On Presentation To:
*30 Minute Release 11i Security -
Keeping The Bad Guys Away*
- Solution Beacon's Security Portal:
www.solutionbeacon.com/security

Case Studies

- Disgruntled Worldcom employee posts stolen names, SSN, birth dates of company executives on public website
- Ex-Employee Steals CRM and Financials Data and Provides to Competitor

Case Studies (cont)

- Employee Sells Credit History Database
- Employee Manipulates Payroll Data
- AOL Employee Sells Email Addresses to Spammer
- Laptops With Sensitive VA Data Stolen

Case Studies (cont)

- Q. What do all of these Case Studies have in common?
 - Disgruntled Employee
 - Ex-Employee Steals CRM and Financials Data
 - Employee Sells Credit History Database
 - Employee Manipulates Payroll Data
 - Employee Sells Email Addresses to Spammer
 - Laptop With Sensitive VA Data Stolen
- A. A firewall didn't help!!!

What is Security?

- What is commonly thought of someone mentions IT “security”?
 - Physical Security
 - Three Gs (Guards, Gates, Gizmos)
 - Technology Stack Security
 - Network (e.g. Firewalls, Proxy Servers)
 - Server (e.g. Antivirus)
 - Database (Auditing?)
 - Application (Access Lists?)

What is Security?

- Most often, Security is focused on trying to keep the *external* bad people out ...
- But who is keeping out the *internal* bad people?

Today's Message

- **The Internal Threats Are Real!**

(Yes, they still are!)

Fact: Internal Threats Are Real

Despite most people's fears that hackers will break into the company and destroy data or steal critical information, **more often than not, security breaches come from the inside.**

Fact: Internal Threats Are Real

- Gartner estimates that more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses ...
- The FBI is also seeing rampant insider hacking, which accounts for 60% to 80% of corporate computer crimes

Fact: It May Happen To You!

- In 2005, 20 Percent of Enterprises Will Experience a Serious Internet Security Incident – Gartner
- In 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated – Gartner

Quotes From Industry Experts

- "Insider attacks are where most of the money's lost, where most of the vulnerabilities are."

Frank Huerta, Vice President Intrusion-Detection Product Delivery, Symantec

- "Technological protection from external threats is indeed important, but human problems cannot be solved with [only] technological solutions."

Eric D. Shaw, Keven G. Ruby, & Jerrold M. Post, Security Awareness Bulletin / RAND

Quotes From Industry Experts

- "In the Banking and Finance sector, fraud is typically perpetrated by a non-technical current or former employee. Sabotage, on the other hand, is typically led by a **technical** disgruntled employee, usually a **former** employee."

Dawn Cappelli, Carnegie Mellon University / CERT / Software Engineering Institute

Fact: It May Happen To You!

- Are you prepared?
- Can you prevent becoming a statistic?

What is Security?

- Security is a **PROCESS** that occurs (or doesn't occur) at multiple levels
- Security awareness at organizations varies due to:
 - Business Core Function
 - Organizational Tolerance (e.g. SOX)
 - Prior Incidents

Security Is A Process

- “Process” means it occurs more than once!
 - Policies, Processes and Procedures
 - Internal and External Checks and Balances
 - Regular Assessments (Focus = Improve)
 - Internal
 - Third Party
 - Audits (Focus = \$ for Auditors)
 - Necessary Evil
 - Many Don’t Understand the Apps

What is Applications Security?

In an Oracle Applications environment, it's protection of information from:

- Accidental Data Loss
- Employees
- Ex-Employees
- Hackers
- Competition

Application Security Is...

- Part Technology, Mostly User Access
- User Security
 - Authentication
 - Authorization
 - Audit Trail

Application Security

- Authentication – Who are you?
- Authorization – What privileges do you have?
- Audit Trail – Effectiveness is almost useless if you can't ensure:
 - Individual accounts are used
 - Individuals are who they say they are

What is “30 Minute Release 11i Applications Security”?

- A Guide to Easily Implement Select Security Controls Consisting Of:
 - User Account Policies
 - Profile Options
- Quick and Easy to Implement
- Low Investment / High Return Value
- “Big Bang for the Buck”
- Required Foundation for other Security Controls

Best Practice: No Shared Accounts

- Difficult or Impossible to Properly Audit
- How Hard Is It To Guess A Username?
- Release 11*i* Feature to Disallow Multiple Logins Under Same Username
- Uses WF Event/Subscription to Update ICX_SESSIONS Table
- 11.5.8 MP
- Patches 2319967, 2128669, WF 2.6

Best Practice: No Generic Passwords

- Stay Away From 'welcome'!!!
 - FNDLOAD and migrating users
- 11.5.10 Oracle User Management (UMX)
 - User Registration Flow
 - Select Random Password
 - Random Password Generator

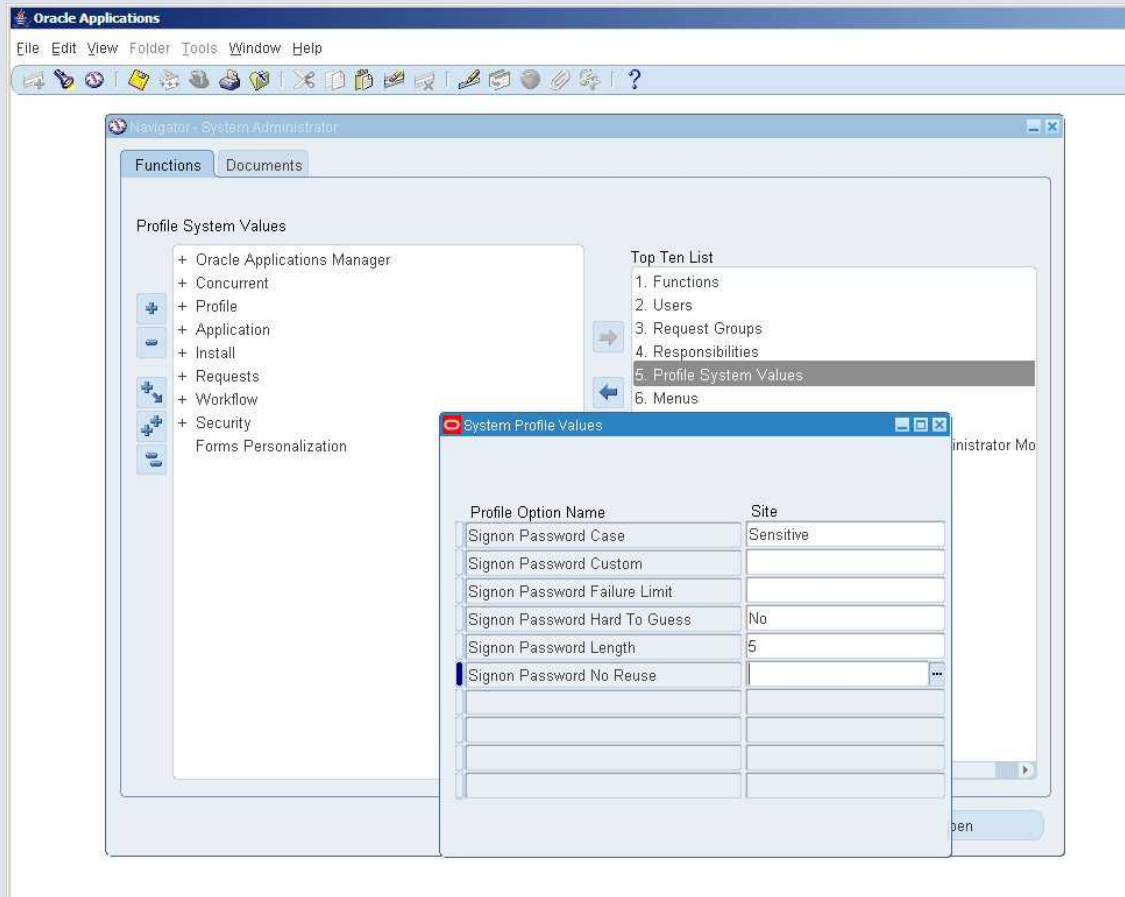
11.5.10 Oracle User Management (UMX)

- UMX leverages workflow to implement business logic around the registration process
- Raising business events
- Provide temporary storage of registration data
- Identity verification
- Username policies
- Include the integration point with Oracle Approval Management
- Create user accounts and release usernames
- Assign Access Roles
- Maintain registration status in the UMX schema
- Launch notification workflows

Best Practice: Set Application User Signon Profile Values

- Signon Password Failure Limit
- Signon Password Hard to Guess
- Signon Password Length
- Signon Password No Reuse
- Signon Password Custom
- Signon Password Case

R12 Signon Password Profiles



Profile: Signon Password Failure Limit

- Default Value = 0 attempts
- Recommendation = 3
- By default, there is no lockout after failed login attempts: This is just asking to be hacked!
- Additional Notes:
 - Implement an alert (periodic), custom workflow or report to notify security administrators of a lockout
 - FND_UNSUCCESSFUL_LOGINS
 - 11.5.10 raises a security exception workflow

Profile: Signon Password Hard to Guess

- The Signon Password Hard to Guess profile option sets internal rules for verifying passwords to ensure that they will be "hard to guess"
- Oracle defines a password as hard-to-guess if it follows these rules:
 - The password contains at least one letter and at least one number
 - The password does not contain repeating characters
 - The password does not contain the username
- Default Value = No
- Recommendation = Yes

Profile: Signon Password Length

- Signon Password Length sets the minimum length of an Oracle Applications password value
- Default Value = 5 characters
- Recommendation: At least 8 characters

Profile: Signon Password No Reuse

- This profile option is set to the number of days that must pass before a user is allowed to reuse a password
- Default Value = 0 days
- Recommendation = 180 days or greater

Profile: Signon Password Custom

- Use if Oracle does not provide the password complexity you need
- Create a custom Java class
- Use the custom class name as the value

Profile: Password Case Option

- Enforces case sensitivity for password values:
 - Insensitive
 - Sensitive
- Introduced in 11i ATG_PF_H RUP3
 - Insensitive
 - Sensitive
 - Mixed
- 11i ATG_PF_H RUP4 deprecated 'Mixed'

Better R11i Security In 3 Days

Keeping The Bad Guys Away

Better R11i Security In 3 Days

- Beyond “Better R11i Security in 30 Minutes”
 - Some New Profiles
 - Additional Best Practices
 - Additional Controls
 - More References
- Keeping the “Badder” guys away!
- Solution Beacon’s Security Portal:
www.solutionbeacon.com/security

Best Practice: Follow Oracle's Best Practice Documents

- 189367.1 Best Practices For Securing the E-Business Suite
- 287176.1 DMZ Configuration With Oracle E-Business Suite 11*i*
- 380490.1 Oracle E-Business Suite R12 Configuration In A DMZ

Best Practice: Protect All of Your Environments

- Secure and Protect Non-Production Instances (e.g. Dev, Test, QA)
- Cloned Databases
- Sensitive Data
- Purge or Obfuscate
- Often have open access (i.e. APPS password gets reset to APPS, or password is publicly known)

Best Practice - No Direct Access to Database

- Protect Your Data!
- No Direct Access to Database
 - Only Allowed Via An Application
 - Does not mean that people can't do their job!
 - Reduces the number of attack vectors
 - Implemented via `tcp.invited_nodes` in `sqlnet.ora`
 - Oracle's Recommendation
 - MetaLink Note: 277535.1

Best Practice - No Direct Access to Database

- No Direct Access (sqlnet.ora) Example:

```
tcp.validnode_checking = YES  
tcp.invited_nodes = (192.168.1.91)  
tcp.excluded_nodes = (192.168.1.89, 192.168.1.90)
```

- In a multi-node/server configuration, the E-Business Web Node, Admin Node, Forms Node and Concurrent Processing Node servers would be included in the list of invited nodes, as well as any other administrative or monitoring servers (e.g. Oracle Enterprise Manager).

R12 OAM Main Dashboard

ORACLE Applications Manager Support Cart Setup Home Logout Help

Applications Dashboard | Site Map

Applications Dashboard: VIS Navigate to Application Services Go

Overview Performance Critical Activities Diagnostics Business Flows **Security** Software Updates

Applications System Status

Data Retrieved: 21-Feb-2007 03:19:19

| Host | Platform | Host Status | Admin | Database | Concurrent Processing | Forms | Web |
|----------|-------------|-------------|-------|----------|-----------------------|-------|-----|
| LARKMEAD | LINUX Intel | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Configuration Changes (last 24 hours)

Data Retrieved: 21-Feb-2007 03:19:19

- Patches Applied 0
- Site Level Profile Options 0
- Applications Context Files Edited 0

System Alerts

Data Retrieved: 21-Feb-2007 03:19:19

- New Alerts 38
- New Occurrences 602
- Open Alerts 0
- Open Occurrences 0

Web Components Status

Data Retrieved: 05-Dec-0006 00:00:00

- PL/SQL Agent ✓ Up
- Servlet Agent ✓ Up
- JSP Agent ✓ Up
- Discoverer ✗ Unmonitored
- Personal Home Page ✓ Up
- TCF ✓ Up

User Initiated Alerts

Data Retrieved: 21-Feb-2007 03:19:19

- New Alerts 0
- New Occurrences 0
- Open Alerts 0
- Open Occurrences 0

TIP The information shown above (with the exception of Web Components Status section) is retrieved from the system periodically. To retrieve up-to-the-minute data, please use the refresh icon for the desired section. Please see Help for more details.

Support Cart Setup Home Logout Help

Copyright 2001, 2006 Oracle Corporation. All Rights Reserved.
 About Oracle Applications Manager Version 2.3.1

R12 OAM Security Dashboard

ORACLE Applications Manager Support Cart Setup Home Logout Help

Applications Dashboard | Site Map

Applications Dashboard: VIS Navigate to Application Services Go

Overview Performance Critical Activities Diagnostics Business Flows **Security** Software Updates

Manage Security Options →

Security Alerts Resources

Last Updated: 21-Feb-2007 03:25:30 Data Retrieved: 07-Dec-2005 07:43:46

| Severity | New | Open |
|----------|-----|------|
| Critical | 0 | 0 |
| Error | 0 | 0 |
| Warning | 0 | 0 |

- Security Announcements and Notes
- Security Announcements and Notes FAQ
- E-Business Suite Security Best Practices
- More ...

TIP Click on the refresh icon to schedule catalog download.

Security Test Failures

Last Updated: 21-Feb-2007 03:25:30

Expand All | Collapse All

| Focus Test Name | Failure Level | Failure Time | Diagnose | Schedule |
|----------------------------|----------------------------|--------------|----------|----------|
| Application Object Library | Error | | Diagnose | Schedule |
| Application Object Library | Application Object Library | | Diagnose | Schedule |

Available Security Related Tests

Last Updated: 21-Feb-2007 03:25:30

Expand All | Collapse All

| Focus Test Name | Last Status | Alert Defined | Diagnose | Schedule |
|--|-------------|---------------|----------|----------|
| Application | | | | |
| CRM Foundation | | | | |
| oracle.apps.jtf.regress.qatool.testcase.AppsPTest | Pass | Warning | Diagnose | Schedule |
| oracle.apps.jtf.regress.qatool.testcase.DBPTTest | Pass | Warning | Diagnose | Schedule |
| oracle.apps.jtf.regress.qatool.testcase.SysAdminRoleTest | Pass | Warning | Diagnose | Schedule |
| Application Object Library | | | | |

R12 OAM – Manage Security Options



Best Practice – Set the Database Listener Password

- Prevent DoS Issues with DB Listener
- Prevent Execution of OS-Level Actions
- Easy to Implement:

```
$lsnrctl  
LSNRCTL> change_password  
Old password: <hit Enter if no prior password value>  
New password: <new password value>  
Reenter new password: <new password value>  
LSNRCTL> save_config
```

Best Practice – Secure Default Accts

- Database Base Accounts (e.g. SYS, SYSTEM)
- Database Product Accounts (e.g. CTXSYS)
- 200+ E-Business Suite Application Accounts (e.g. APPS, APPLSYS, GL, MFG, etc.)
- Demonstration Accounts (e.g. SCOTT, QS, QS_ADM, etc.) should be dropped
- Lock and Expire most of the remaining:

```
alter user OUTLN identified by gr#8w1n3s  
account lock password expire;
```
- All of the above accounts and default passwords are well known to internal and external bad guys!

Best Practice - Force Apps User Passwords To Expire

- By default, passwords do not expire
- Define User screen – Password Expiration
 - Days
 - Accesses
 - None (Default)
- Unfortunately, no global setting

R12 Define Users Screen

Oracle Applications

File Edit View Folder Tools Window Help

Users

User Name:

Password:

Description:

Person:

Customer:

Supplier:

E-Mail:

Fax:

Password Expiration

Days

Accesses

None

Effective Dates

From:

To:

Direct Responsibilities | Indirect Responsibilities | Securing Attributes

| Responsibility | Application | Description | Security Group | Effective Dates From | Effective Dates To |
|----------------------|----------------------|-------------|----------------|----------------------|--------------------|
| System Administrator | System Administrator | | Standard | 18-FEB-2007 | |
| | | | | | |
| | | | | | |
| | | | | | |

Best Practice: Configure Additional Security-Related Profile Options

- Sign-On: Audit Level
- Sign-on: Notification
- Utilities: Diagnostics
- FND: Diagnostics
- Hide Diagnostics
- Concurrent: Report Access Level
- AuditTrail: Activate

Profile Sign-On: Audit Level

- Defines what level the system will perform auditing for “user navigation”.
- Levels
 - User
 - Responsibility
 - Form
- Note that the ‘audit content’ only captures information about What the users’ navigation was during a session based on the Audit Level, it does not audit what occurs while a user is on a form, for example.

Diagnostics Profiles

- **Utilities:Diagnostics**

Allows Forms users to examine (and change) individual database records. Set this to "No" so that APPS password is required before using this capability.

- **FND:Diagnostics**

This is the Self Service equivalent of Utilities:Diagnostics.

- **Hide Diagnostics**

Setting this option to Yes hides the diagnostics menu from users.

Profile Concurrent:Report Access Level

- Set this profile option to 'User' to restrict a user from viewing other users' concurrent requests.

Profile Audit Trails Activate Yes for the EBS auditing to function

Best Practice – Change Passwords Frequently!

- apps, applsys, gl, ap, ar, etc.
- FNDCPASS - MetaLink Note: 159244.1
- 'ALLORACLE' mode – 11i.ATG_PF.H RUP4
 - Changes all E-Biz Oracle passwords
 - Exception: apps and applsys
 - I don't necessarily encourage its use

Notes On Oracle DB Password Values

- If the password is not enclosed in quotes then it can include any letter, any digit, or any of the three following special characters: "_", "#", or "\$".
- Only a letter can be used in the first character, the other characters can be used after that.
- It is important to remember that Oracle passwords are not case sensitive so the valid alphabet is reduced by 26 characters. That is "a" is the same as "A".

Best Practice – Set Tech Stack Timeout Parameters

- Profiles and Configuration Parameters
 - ICX Timeout Profiles
 - CRM Application Profiles
 - Jserv (Java) Timeout Settings
 - Apache HTTP Timeout Settings
 - Forms 60 Environment
 - Oracle Single Sign On Timeout Settings
- Refer to whitepaper for detailed information – will provide one here...

Profile: ICX:Session Timeout

- The length of time (in minutes) of inactivity in a user's form session before the session is *disabled*.
- Default value = none
- Recommendation = 30 (minutes)
- Also set *session.timeout* in *zone.properties*
- Available via Patch 2012308
(Included in 11.5.7, FND.E)

Best Practice – Restrict Forms That Allow SQL Input

- Some forms allow users to input SQL statements!
- This is a serious attack vector that needs to be eliminated or severely restricted!
- Need to audit the affected tables if allowed
- Review whitepaper for specifics (Form Function, Form Name, and Table Name)

Day 4 – Your Next Steps

- Be Paranoid!
- Review/Update/Create Your Security Processes, Procedures and Policies
- Be Proactive – Monitor Security Sources
 - CERT (OS, products, and more)
 - Oracle
- Be Proactive – Apply Oracle Critical Patch Updates
 - Quarterly Releases
 - Not Cumulative!
 - Make CPUs part of Release Management Process
 - April 17, 2007
 - July 17, 2007

E-Business Suite Critical Patch Update Note 372931.1

- Introduced in the October 2006 Critical Patch Update (CPUOct2006), the **minimum supported baseline** for Oracle E-Business Suite Release 11.5.10.x is be Oracle Applications Technology **11i.ATG_PF.H RUP3** (4334965).
- The 11.5.10 CU2 for ATG Product Family is **no longer** a supported baseline. The minimum supported baseline for all other 11i releases, including 11.5.7, 11.5.8, and 11.5.9, is the patch levels listed in Note 363827.1

E-Business Suite Critical Patch Update Note 372931.1

- Oracle recommends that all Release 11*i* customers uptake Oracle Applications Technology 11*i*.ATG_PF.H Rollup 4 (4676589).
- Beginning with the July 2007 Critical Patch Update (CPUJul2007), Oracle Applications Technology will support only the current and previous production rollups (RUP N and **RUP N-1**) as patching baselines for all 11*i* releases.
- CPU FAQ 360470.1

Day 4 – Your Next Steps (continued)

- Harden Operating System
- Harden Database
- Harden E-Business Suite Tech Stack
- Continuous Process Improvement
 - Internal Assessment
 - Third Party Assessment
- Implement Other Best Practices
 - Solution Beacon's Security Portal:
www.solutionbeacon.com/security

Questions?

- Answers
- Lies
- Untruths

Thank you!

Randy Giefer

rgiefer@solutionbeacon.com

www.solutionbeacon.com

Real Solutions for the Real World.[®]

Visit Our **Booth #339**
to Register for a
***World Class
Weekend Trip!***

Got Oracle? Get the Book!

Installing, Upgrading
and Maintaining
Oracle E-Business Suite
Applications 11.5.10+

It's available in
the OAUG Bookstore
or online!

Sign up for the
Solution Beacon Newsletter
www.solutionbeacon.com

