



OAUG®

TRAIL TO TEXAS



30 Minute Release 11/Security... *Keeping the Bad Guys Away*

Session Leader
John Stouffer, Solution Beacon

Compiled by Randy Giefer, Solution Beacon

TRAIL to TEXAS sm

Release 11/Workshops

NorCal OAUG / San Ramon, CA • NEOAUG / Worcester, MA •
SROAUG / Los Angeles, CA • CSOAUG / St. Louis, MO •
IOUG / Orlando, FL •

www.solutionbeacon.com

ORACLE CERTIFIED PARTNER

© 2005 Solution Beacon, LLC. All Rights Reserved.



Agenda

- Welcome
- Presenter Introduction
- Presentation Overview
- 30 Minute R11/Security
- Audience Survey
- Questions and Answers

30 Minute Release 11/Security

“Keeping The Bad People Away”

■ Case Studies

- ◆ Disgruntled employee posts names, SSN, birth dates of company executives on website
- ◆ Ex-Employee Steals CRM and Financials Data and Provides to Competitor
- ◆ Employee Sells Credit History Database
- ◆ Employee Manipulates Payroll Data
- ◆ Employee Sells Email Addresses to Spammer

30 Minute Release 11/Security “Keeping The Bad People Away”

- 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

- A. A firewall didn't help!!!

What Is Security?

- What do you think of when someone mentions “security”?
 - ◆ Physical Security
 - ◆ Three G’s (Guards, Gates, Gizmos)
 - ◆ Technology Stack Security
 - ◆ Network (e.g. Firewalls)
 - ◆ Server (e.g. Antivirus)
 - ◆ Database (Auditing?)
 - ◆ Application (?)

What Is Security?

- Network / Perimeter Security
 - ◆ Firewalls
 - ◆ Proxy Servers
 - ◆ Encrypted Traffic
- Designed to keep the *external* bad people out ...
- Who is keeping out the *internal* bad people?

Today's Message

- Internal Threats Are Real !!!

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

- Through 2005, 20 Percent of Enterprises Will Experience a Serious Internet Security Incident – Gartner
- By 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated – Gartner
- Are you prepared?
- Can you prevent becoming a statistic?

What Is Security?

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

Security Is A Process

- “Process” means it occurs more than once!
 - ◆ Processes and Procedures
 - ◆ Internal and External Checks and Balances
 - ◆ Regular Assessments (Focus = Improve)
 - ◆ Internal
 - ◆ Third Party
 - ◆ Audits (Focus = Identify Problems)

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

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

Application Security

- 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 R11/ Applications Security?

- Checklist to Easily Implement Two Types/Categories of Security:
 - ◆ User Account Policies
 - ◆ Profile Options
- Quick and Easy to Implement
- Low Investment / High Return Value
- “Big Bang for the Buck”

Best Practice: No Shared Accounts

- Difficult or Impossible to Properly Audit
- How Hard Is It To Guess A Username?
- Release 11/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'!!!
- 11.5.10 Oracle User Management (UMX)
- 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
- Release usernames
- Assign Access Roles
- Maintain registration status in the UMX schema
- Launch notification workflows

Profile: Signon Password Length

- Signon Password Length sets the minimum length of an Oracle Applications password value
- Default Value = 5 characters
- Recommendation: At least 7 characters

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 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 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 will raise a security exception workflow

Profile: ICX:Session Timeout

- This profile option determines the length of time (in minutes) of inactivity in a user's form session before the session is *disabled*. Note that disabled does not mean terminated or killed. The user is provided the opportunity to re-authenticate and re-enable their timed-out session. If the re-authentication is successful, the disabled session is re-enabled and no work is lost. Otherwise, the session is terminated without saving pending work.

Profile: ICX:Session Timeout (cont.)

- Default value = none
- Recommendation = 30 (minutes)
- Also set *session.timeout* in *zone.properties*
- Available via Patch 2012308
(Included in 11.5.7, FND.E)

Wrap Up

- Remember: The Internal Threat Is Real
- Thanks to OAUG and to CSOAUG
- Thank *you* for attending!

John Stouffer
jstouffer@solutionbeacon.com