

✓ INTEGRITY ✓

Mission Critical Applications...
...Mission Critical Security



NCOAUG Training Day 2005

The Basics of Installing & Running Oracle Applications Securely

Stephen Kost

Chief Technology Officer
Integrigy Corporation

Integrigy Background

- **Extensive experience with Oracle Applications**
 - Founded by former Big-6 consultants with significant experience on Oracle Applications implementations in Fortune 500 companies
 - Founders recognized a major gap in all implementations – little or no security auditing done on projects
 - Integrigy has found more security bugs in Oracle Applications than anyone else inside or outside of Oracle
- **An Oracle Applications company first, a security company second**
 - Products developed to support and enhance an Oracle Applications implementation – Integrigy understands the issues and risks challenging large Oracle implementations

Security Perspective

- Goal is to improve security, can't make it perfect
- Security is a cost/benefit proposition
 - Risks and threats must be understood
- Balance security objectives with operational realities
- Perimeter network is secure, but internal network is open and insecure
- Internal threat is greater than external threat
 - Insider knowledge and understanding of Oracle Applications is far greater and more dangerous
- If someone wants in, they can get in

Security Perspective

- **Undisclosed security holes exist in Oracle**
 - Integrity has 36 security bugs in process with Oracle
 - Other security vendors have 55+ open Oracle security bugs
 - Time from discovery to patch release may be 3 to 24 months
- **Oracle's security focus is on 11.5.9 and 11.5.10**
 - Best practices document is for 11.5.9 (with many patches)
 - Secure coding standard mandated with 11.5.9 and onward
- **“Unbreakable” marketing campaign does not include Oracle Applications**
 - Nor does it include 8.1.7 and 9iAS 1.0.2.2
 - Oracle Applications is not externally audited for security

Oracle Applications Overview

- **Oracle Applications is massive and complex**
 - Millions of lines of code, multiple programming languages
 - Evolutionary development over 17 years, lots of legacy code
- **Multiple technologies are involved**
 - Networks, Operating System, Web sever (Apache), Application Server (Forms, JServ, JSP), Database (Oracle), Reporting, etc.
- **DBAs and system admins have little time for security**
- **Oracle Applications is often customized or extended**
- **Security tasks and testing are often late in the application implementation life-cycle**

Security Challenges

- Oracle Applications provides “foot in the door” with the **APPLSYSPUB** and **GUEST** accounts
- No granularity in database model – **APPS** account
- Many default account passwords and default configuration settings that are not secure
- Poor segregation of system administration duties
- Too many “Keys to the Kingdom”
 - UNIX – **root, oracle, applmgr**
 - Database – **system, sys, apps, applsys**
 - Applications – any account with **sysadmin** responsibility

Installation

- **All products and modules installed by default**
 - In 11.5.10, 200+ modules are installed even if only a few are used
- **Limit access to the database server**
 - Use a firewall on the data center perimeter
 - Use valid node checking (see Metalink 291897.1)
 - Set password on database listener ★
- **Apply the newest certified patchsets and apply latest security patches**
 - Use 9.2.0.x instead of 8.1.7.4
 - Apply most recent FND Patchset

Integrigy Oracle Apps Security Alerts

- **Critical Patch Update January 2005 – 11.0.x, 11.5.1 – 11.5.9**
 - 8 SQL Injection vulnerabilities (patches available since June 2002)
- **Oracle Security Alert #67 – 11.0.x, 11.5.1 – 11.5.8**
 - 10 SQL injection vulnerabilities
- **Oracle Security Alert #56 – 11.0.x, 11.5.1 – 11.5.8**
 - Buffer overflow in FNDWRR.exe
- **Oracle Security Alert #55 – 11.5.1 – 11.5.8**
 - Multiple vulnerabilities in AOL/J Setup Test JSPs
 - Obtain GUEST password, server key, and valid session
- **Oracle Security Alert #53 – 10.7 - 11.5.8**
 - No authentication in FNDFS program
 - Retrieve any file from O/S

Upgrading

- **Oracle adds, but rarely removes**
 - Many upgrade “artifacts”, especially with major version upgrades (e.g., 10.7 to 11i)
 - New products introduced in every version
- **After an upgrade –**
 - Check for new database and application users ★
 - Check for database and application user passwords reset to default values (i.e., CTXSYS)
 - Remove obsolete customizations after major version upgrades

Configuration (Top 4)

- **Change default database account passwords** ★
 - 200+ default passwords must be changed
- **Change default application account passwords** ★
 - 20+ default passwords must be changed and most disabled
- **Use AutoConfig – fixes many security issues in the configuration files**
 - AutoConfig Template Patch E (August 2003) or greater
 - Included with 11.5.10 and FND.H
- **Set security related profile options**
 - Map internal security policies to the profile options

Auditing

➤ No default auditing

- By default, no information on database connections, application logins, responsibilities, or forms access

▪ Setup database auditing

- At least, audit sessions, users, database links, and auditing ★

▪ Use Oracle Applications AuditTrails only for non-transaction tables or use a third party tool

- Auditing heavily used tables can impact performance
- At least, audit critical FND tables

▪ Set profile option “Sign-On Audit Level” to “FORMS” ★

- Audits logins, responsibilities, and forms usage

▪ See Integrigy’s “Guide to Auditing in Oracle Applications” for more detailed recommendations

User Management

- **No generic or shared accounts**
 - Often used for execution of scheduled concurrent programs
- **No default passwords for new accounts (i.e., welcome)**
 - Usually between 10-35% of accounts are never used
- **Expire unused accounts on a periodic basis**
- **Check how many accounts have system administrator responsibility or access to sysadmin functions**
- **For new implementations in 11.5.10, use the new “User Management” functionality**
 - Upgrades to 11.5.10 should use the new registration, password reset, delegation, and approvals functionality, but only consider the roles functionality if needed

Customizations and Change Mgmt

- **Check the APPLSYSPUB permissions ★**
 - Inappropriate grants and objects
 - Check for PUBLIC database links
- **Perform code reviews on all customizations**
 - Coding standard should be no dynamic SQL, use bind vars
 - Look for echoing of APPS password in shell scripts
- **No developer access to production**
- **Check passwords on all custom database accounts**
- **No APPS_READ or similar accounts**
- **Use severely limited accounts for interfaces**

References

- **Oracle “Best Practices for Securing Oracle E-Business Suite 3.0.1” – Metalink Note 189367.1**
 - Many sections written by Integrigy
 - Comprehensive, but contains errors and omissions
 - Assumes at least 11.5.9 with many patches
- **Integrigy Security Guides (www.integrigy.com)**
 - “Guide to Auditing in Oracle Applications”
 - “Oracle Applications 11i Security Quick Reference”
 - “Oracle Database Listener Security Guide”
 - Integrigy security alerts and advisories
 - Previous conference presentations

Integrigy's Products and Services

AppSentry™

- Security scanner for databases, application servers, and ERP packages
- Performs advanced penetration testing and in-depth security and controls auditing – performs over 300+ audits and checks on Oracle products
- Runs on any Windows PC and requires no software to be installed on the target servers

AppDefend™

- Application firewall and intrusion prevention system for ERP packages
- Blocks common attacks like SQL injection, session hijacking, and cross site scripting
- Blocks access to unimplemented Oracle Applications modules

Oracle Applications Security Assessments

- On-site security assessments of Oracle Applications (fixed fee and fixed duration)
- All aspects of the technical infrastructure are assessed from the technology stack (database, application server, and applications) to operational procedures to customizations.

Contact Information

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681
888/542-4802

Website: www.integrigy.com

Sales: sales@integrigy.com

Development: development@integrigy.com

Support: support@integrigy.com

Security Alerts: alerts@integrigy.com

Copyright © 2005 Integrigy Corporation. All rights reserved.