



Security Best Practices

IT Security Best Practices in an Oracle Applications Environment

Stephen Kost

Chief Technology Officer
Integrigy Corporation

Agenda

- **General Oracle Security**
- **Oracle Applications SOX IT Challenges**
- **SOX Technical Compliance Model**
- **Oracle Security Patches (CPUs)**

Oracle Security Perspective

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
- Developer security only now happening
- **“Unbreakable” marketing campaign does not include Oracle Applications**
 - Nor does it include 8.1.7 and 9iAS 1.0.2.2.x
 - Oracle Applications is not externally audited for security
- **Undisclosed security holes exist in Oracle**
 - Integrigy has open 11i security bugs in process with Oracle
 - Security researchers have 100+ open Oracle security bugs

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**

Oracle 11i Security Weaknesses – Top 5

- Oracle Applications provides “foot in the door” with the **APPLSYS** and **PUB** and **GUEST** accounts
- Many default account passwords and default configuration settings that are not secure
 - Especially prior to 11.5.10
- All products and modules installed by default
 - In 11.5.10, 250+ modules are installed even if only a few are used
- Oracle adds, but rarely removes
 - Many upgrade “artifacts” from minor (e.g., 11.5.5 → 11.5.10) and major upgrades (e.g., 10.7 → 11i)
- Customizations result in many security issues
 - 40% of all security issues identified during our audits are related to customer customizations

IT Security Challenges

- No granularity in database model – **APPS** account
- **APPS** account used for all end-user access and most administration (adpatch, adadmin, etc.)
- 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

IT Security Challenges

- **No auditing enabled by default**
 - Only creation and last update audited, no history
 - Auditing must be done at both the database and application level
 - Potential severe performance issues if auditing is not carefully designed – must including purging and reporting in design
- **Oracle Applications provides no inherent controls for change management**
 - “California” style of management for changes
 - Customer must implement extensive policies and procedures and/or third party products
- **Generic accounts often used to simplify management and operations**

Operational Security Domains

		Oracle Applications Technical Components			
		Oracle Applications	Database	Application Server	Operating System
Operational Processes	1. Security	1.1 User Management	1.3 Database Security	1.4 Network and Web	1.5 OS Security
		1.2 Segregation of Duties			
	2. Auditing	2.1 Application Auditing	2.2 Database Auditing	2.3 Web Logging	2.4 OS Auditing
	3. Monitoring and Troubleshooting	3.1 Application	3.2 Database	3.3 Web and Forms	3.4 Operating System
	4. Change Management	4.1 Object Migrations	4.3 Change Control	4.5 Change Control	4.6 Change Control
		4.2 Application Configuration	4.4 Database Configuration		
5. Patching	5.1 Application Patches	5.2 Database Patches	5.3 Application Server Patches	5.4 OS Patches	
6. Development	6.1 Application	6.2 Database	6.3 Web	6.4 Shell and File Transfer	

Oracle Security Patches

- Fixes security bugs in the Oracle Database, Oracle Application Server, Oracle Applications, and other Oracle products
- Types of security bugs typically fixed by a security patch –
 1. Buffer Overflows
 2. SQL Injection
 3. Permission Issues
 4. Denial of Service
 5. Cross Site Scripting
- Security patches are released as Critical Patch Updates on a quarterly basis – 6 so far = 200+ security bugs
 - CPU includes anywhere from 20 to 70 bugs fixes
 - Next CPUs – July 18, 2006 and October 17, 2006

Integrigy Security Alerts

- **Critical Patch Update October 2005 – 11.0.x, 11.5.1 – 11.5.10**
 - Default configuration issues
- **Critical Patch Update July 2005 – 11.0.x, 11.5.1 – 11.5.10**
 - SQL injection vulnerabilities, information disclosure
- **Critical Patch Update April 2005 – 11.0.x, 11.5.1 – 11.5.10**
 - SQL injection vulnerabilities, information disclosure
- **Critical Patch Update January 2005 – 11.0.x, 11.5.1 – 11.5.10**
 - SQL injection vulnerabilities
- **Oracle Security Alert #68 – Oracle 8i, 9i, 10g**
 - Buffer overflows and listener information leakage
- **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

Security Patch Process

Bug reported

Security researcher or customer reports bug to Oracle

- Currently, 100-200 open bugs reported by a number of independent security researchers

Oracle researches bug

Oracle develops bug fix

- Finder not allowed to test fix or even notified about fix

Oracle may include fix in new releases and patch sets

- No notification of security fixes to customers

Oracle includes fix in quarterly CPU

From report to security patch release is 6 months to 3 years

- Bugs are rarely fixed in under 6 months
- Time to fix is not decreasing with move to CPUs

Elapsed time on average is 18 months

Bug fixed



Security Patch Issues

- **Oracle is forcing customers to upgrade technology stack components in order to apply security patches**
- **Independent security researchers have reported the following issues with Oracle Database and Oracle Application Server patches –**
 - **A few patches don't update the correct files – an Oracle QA issue**
 - Difficult to thoroughly test patches for all versions and platforms
 - **Some fixes for security bugs are not robust**
 - Simplistic fixes applied – only address exploit, not true problem
- **Integrigy reviews and tests Oracle Applications 11i patches**
 - **No major issues found to date**

Security Patch Advice

■ General advice –

- Apply the Database patch – cumulative for all CPUs and previous security alerts
- Apply Oracle Applications patches – not cumulative, must apply all patches from all previous CPUs
- Evaluate the effort to apply Developer 6i, Application Server, and JInitiator patches – depending on risk and effort, delaying these patches may be warranted

■ Specific advice –

- Integrity releases guidance for each CPU on our website
- Each CPU has unique issues and requirements, thus need to be evaluated independently

References

- **Oracle “Best Practices for Securing Oracle E-Business Suite 3.0.2” – Metalink Note 189367.1**
 - Many sections written by Integrigy (see page ii)
 - Assumes at least 11.5.9 with many patches
 - Comprehensive, but contains some errors and omissions
- **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
 - Conference presentations

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

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 © 2006 Integrigy Corporation. All rights reserved.