

# ✓ INTEGRITY ✓

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

# ***Securing 11i: What Did You Miss?***

**Stephen Kost**

*Chief Technology Officer  
Integrigy Corporation*

# Security Perspective

---

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

# Oracle Applications Security 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 administrators have little time for security
  - No comprehensive and complete security documentation
- Oracle Applications is often customized or extended
- Testing and security tasks are often late in the application implementation life-cycle

# Oracle Applications Security Issues

---

- Oracle Applications provides “foot in the door” with the **APPLSYSPUB** and **GUEST** accounts
  - Many functions and features require only an Apps session
- 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
- Minimal default auditing or logging
- Too many “Keys to the Kingdom”
  - UNIX – **root, oracle, applmgr**
  - Database – **system, sys, apps, applsys**
  - Applications – any account with **sysadmin** responsibility

# Oracle Applications Security

---

- Connect as **APPLSYSPUB/PUB** and browse the database using a query tool like TOAD
  - Look at APPLSYSPUB, APPS, APPLSYS, SYS, and custom schemas
  - Check for public database links
- Login as **GUEST/ORACLE** (or GUEST/GUEST)
  - What responsibilities does GUEST have?
- Change passwords and disable unused default Oracle Applications accounts (10-15 accounts)
  - **ASGADM, MOBILEADM, OP\_SYSADMIN** may have system administrator responsibility
  - Check for new accounts added during upgrades
  - **Default passwords can be used to decrypt APPS password**

# Security Related Profile Options

---

## Signon Profile Options

- Signon Password Length
- Signon Password Hard to Guess
- Signon Password No Reuse
- Signon Password Failure Limit
- Sign-on: Audit Level
- Sign-on: Notification

## Other Profile Options

- Utilities: Diagnostics (Forms)
- Hide Diagnostics menu entry (Forms)
- FND: Diagnostics (Self-Service)
- ICX: Session Timeout

# Integrigy Security Alerts

---

- **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
- 10+ more security alerts currently “in process” with Oracle

# Database Security Issues

---

- Database model, init.ora parameters, configuration, and schemas determined by Oracle and should not be changed
  - 200+ standard database accounts and schemas
  - Password management rules can not be used
  - Public access to all standard database packages including UTL\_FILE, UTL\_HTTP, UTL\_TCP, DBMS\_PIPE, etc.
  - **Init.ora - O7\_DICTIONARY\_ACCESSIBILITY = TRUE**
  - Init.ora – AUDIT\_TRAIL = FALSE
  - Init.ora – \_TRACE\_FILES\_PUBLIC = TRUE
  - No auditing by default
- Multiple vulnerabilities and security issues exist with the Oracle database listener
  - Default listener configuration (listener.ora) is not secure
  - **No listener password is set by default – anyone can shutdown listener or set a listener password**

# Database Security

---

- Limit direct access to the Oracle Database
  - Only DBAs and system administrators
  - No Read accounts (APPS\_READ) or extremely limited
  - Oracle Applications passwords can be decrypted
- Review all Oracle database accounts
  - Remove all developer and non-product accounts from production
- Change passwords on all Oracle database accounts
  - Change **SYS** and **SYSTEM** passwords
  - Review documentation for changing **APPS**, **APPLSYS**, **CTXSYS**, and **DBSNMP** passwords
  - Use SQL script to generate **FNDCPASS** script
  - Not necessary to change **APPLSYSPUB** account
  - **Be aware of third party product accounts**

# Database Security

---

- Review all Public and **Applsyspub** privileges
  - Check access to all objects including packages and tables against freshly installed instance
  - **<FND\_TOP>/admin/sql/afpub.sql** has default permissions for **APPLSYSPUB**
  - **Concentrate on custom developed objects and schemas**
- Review all database links in production and development environments
  - Often used to migrate code and FSGs
- Turn on session level auditing
  - Audit all session connections (audit session;)
  - Provides connection and performance information

# Application Server Issues

---

- Multiple products with different configuration files and options
- Oracle iAS installed with all demos and samples by default
- Default Apache configuration should be configured to be more secure
- **AutoConfig makes modifying configuration for enhanced security very difficult**
  - Any changes to configuration files may be overwritten by AutoConfig

# Application Server - Apache

---

- Remove all Apache and iAS demos
  - Review **oracle\_apache.conf** to determine locations
  - Remove default Apache CGI-Bin programs
- Turn off directory indexing in **httpd.conf**
- **Oracle Security Alert #36** –11.5.1 – 11.5.8
  - Apache Chuck Encoding vulnerability
  - Apply Patch 2424256 or 2674529 depending on version
- Upgrade from Apache 1.3.9 to 1.3.12 or iAS 1.0.2.2
  - 11.5.1 – 11.5.6 only, Metalink Note ID 161779.1
- Place **robots.txt** file in \$OA\_HTML to prevent indexing by search engines

# Application Server - Modplsql

---

- Verify that the Oracle Applications modplsql custom authentication package is working properly
  - `http://<hostname>:<port>/pls/<dad_name>/HTP.HR` should return an error or prompt for a password
  - Execute `$FND_TOP/admin/sql/AFOAUTHB.pls` to reload custom authentication package if necessary
- Verify that the **modplsql** admin pages are not accessible
  - `http://<hostname>:<port>/pls/admin_/`

# Customizations

---

- Many security issues and vulnerabilities are the result of customizations
- Review all custom database objects for grants to ALL or PUBLIC
  - Accessible by APPLSYSPUB
- Review custom code for security issues
  - Dynamic SQL statements are vulnerable to SQL injection - **DBMS\_SQL**, **EXECUTE IMMEDIATE**, dynamic cursors
- All interfaces (database links or FTP) should use limited database or UNIX accounts
  - Never use applmgr, APPS, or anonymous FTP for inbound
- Check shell scripts for use of the APPS password
  - Use ENCRYPT in concurrent program options

- **Application Security Assessment tool for the Oracle E-Business Suite**
  - In-depth security and controls auditing
  - Validates security of network, operating system, web server, database, and application
    - Advanced penetration testing
    - Scanning of open network ports for well-known and application specific vulnerabilities
  - Validation of application and technology stack configuration by analyzing configuration files, logs, and file versions
  - Understands the unique technology stack, data model, and application design of Oracle Applications
  - Runs from a PC, nothing installed on the servers

# AppSentry™ Oracle 11i Audits and Checks

---

- **300+ Checks in Operating System, Web Server, Application Server, Database, and Application**
- **Operating System**
  - Standard Oracle accounts
  - UNIX and Windows security patches
- **Web Server**
  - Apache configuration (http.conf)
  - Apache logging (http.log)
  - Apache virtual directories
  - Apache and JServ security patches
  - SSL configuration
  - Oracle support cgi-bin scripts
  - PLSQL Cartridge exploits
- **Application Server**
  - Forms and reports security patches
  - SSL configuration
- **Database**
  - Database accounts
  - Listener exploits
  - Database auditing (SYS.AUD\$)
  - Database security patches
  - APPS permissions
  - APPLSYSPUB permissions
  - Database links
- **Oracle E-Business Suite**
  - Application accounts
  - Users with Sysadmin responsibility
  - Application's security patches
  - Application auditing
  - Password related profile options

- **Application intrusion prevention system for the Oracle E-Business Suite**
  - Scans all incoming web requests for common web application vulnerabilities including –
    - SQL Injection, Cross Site Scripting, Buffer Overflows, etc.
  - **Permits access to only enabled/installed Oracle Applications Modules**
    - Oracle Applications delivered with 12,000 accessible Java Server Pages and Java servlets, even though only a 1,000 or fewer may be used by the customer
  - Blocks unused CGI-Bin programs and sample applications
  - Users can specify filters to block other programs or files
  - Blocks published and un-published Oracle Applications security vulnerabilities

# Additional Information

---

- [www.integrigy.com](http://www.integrigy.com)
  - Oracle Applications 11i Security Quick Reference
  - Guide to Auditing in Oracle Applications
  - Oracle Database Listener Security Guide
  - Integrigy Security Alerts
  
- Oracle
  - Best Practices for Securing Oracle E-Business Suite –Metalink Note ID 189367.1
  - Best Practices for Securing Oracle E-Business Suite for Internet Access – Metalink Note ID 229335.1
  - 11i: A Guide to Understanding and Implementing SSL for Oracle Applications – Metalink Note ID 123718.1
  - Oracle Applications 11i System Administrator's Guide
  - Oracle Security Alerts – <http://technet.oracle.com>

---

***Questions?***

---

## Presenter

Stephen Kost  
Chief Technology Officer  
Integrigy Corporation  
stephen.kost@integrigy.com  
(312) 593-4333

Copyright © 2004 Integrigy Corporation. All rights reserved.

## Integrigy Corporation

2052 Lincoln Park West, Suite 1301  
Chicago, Illinois 60614  
(888) 542-4802  
(312) 242-1798 fax

<http://www.integrigy.com>

Sales: sales@integrigy.com  
Development: development@integrigy.com  
Support: support@integrigy.com  
Security Alerts: alerts@integrigy.com  
Alert Newsletter: newsletter@integrigy.com