

✓ INTEGRITY ✓

***Mission critical applications...
mission critical security!***

Securing the Oracle Applications Infrastructure

Oracle AppsWorld

Stephen Kost

Chief Technology Officer

Integrigy Corporation

Abstract

The infrastructure underlying Oracle Applications is often not well understood and thus sometimes not properly secured. Networks, Web servers, application servers, and databases need to be carefully reviewed to ensure an environment that is well protected against both internal and external attacks.

Most database and application administrators are not familiar with the nuances of networks and Web servers and need to know how to properly configure all the Oracle products to implement a secure infrastructure.

This presentation explains in detail security implications and issues related to deploying the Oracle Applications 11.0 and 11i infrastructure. It provides guidelines for configuring security in Web servers, application servers, databases, and Oracle Applications. It also covers a security model for custom-developed components, including interfaces and database links.

Topics

- Security Introduction
- Operating System – UNIX
- Web Servers
- Applications and Forms Servers
- Oracle Database
- Oracle Applications
- Custom Development

Scope

- Goal is to improve security, can't make it perfect in 1 hour
- Oracle Applications 11.0 and 11i
- Focus on UNIX-based systems
 - Windows 2000 and NT have different security issues
- Focus on “average” business
 - Not military, government, or other organizations that may require highly secure implementations
- Does not include Internet connected applications
 - Self-Service, iProcurement, etc.
- Does not include CRM
- Does not include Oracle Applications security
 - Menus, functions, responsibilities, etc.

Who and Why?

- Revenge (internal)
 - Terminated or disgruntled employees
- Profit (external/internal)
 - Credit card numbers
 - Financial results prior to public announcement
 - Fraud
- Espionage (external)
 - Corporate theft of competitive data
 - Price lists
 - Customer lists
- Terrorism and Vandalism (external)

How? Points of Entry

- “Software Flaws”
 - Bugs or design flaws in delivered software
 - All software has exploitable flaws
- “Default and Bad Configuration”
 - Well-known default software configuration settings such as default usernames and password
 - Error in the configuration can create holes
- “Revelation”
 - Security measures are compromised through revelation of passwords or other information
- “Added Flaws”
 - Customizations result in exploitable flaws

Attacks

- The best attack is an undetected attack
 - Steal or compromise information without detection
- External attacks tend to be bottom-up
 - Penetrate network, then UNIX or web server, then application
- Internal attacks tend to be top-down
 - Immediately penetrate application
- Organization must be prepared to quickly respond to attacks
 - Security plan and policy must be in place prior to an attack

Problems with Security

- Security vs. Performance
 - Auditing and other security features do impact and decrease system performance
- Security vs. Productivity
 - Security does limit individual productivity
- Security vs. Maintenance
 - Additional maintenance and monitoring is required for good security
- Security vs. Organizational Structure
 - Security often crosses organizational structures and requires consensus

Creating Security

- Well-documented Security Plan and Policy
 - Created at beginning of project
 - Covers all aspects from operating system, web servers, databases, application, development, networks, to disaster recovery
 - Includes a security model for development
- Security Audit
 - Complete audit 30-60 days prior to go-live
 - Additional audit around go-live
 - Periodic audits every 6-12 months by external team
- Check Metalink, Technet, and other websites for security alerts

***You must make Oracle
Applications secure!***

Oracle Apps Issues

- Complex environment with multiple products and technologies
- DBAs are sometimes responsible for UNIX and web server security
- Oracle Apps provides “foot in the door” with the APPLSYSPUB account
- Lack of security granularity within Oracle Applications
- “Keys to the Kingdom”
 - UNIX – root, oracle, applmgr
 - Database – system, sys, apps, applsys
 - Applications – any account with system administrator responsibility

Default Accounts

Layer	UNIX	Web, Forms, Application Servers	Oracle Database
Product			
Web, Forms, Application Servers	oracle applmgr	admin	www_user, www_dba
Oracle Database	oracle		system, sys, ctxsys, dbsnmp, rman, scott, mdsys, ordsys, demo
Oracle Applications	applmgr		apps, apps_mrc, applsys, applsyspub, 50+ more
Third Party			noetix_sys, vertex_login, perfstat, cli

Default Ports

Product	Ports
Oracle Database 8.0.x and 8i	1521
Oracle Web Application Server 3.0.2	8888, 80, 2649 (UDP)
Oracle Application Server 4.0.x	80, 443 (SSL)
Oracle iAS – Apache Listener	7777, 80, 443 (SSL)
Oracle Forms Server	9000
Oracle WebDB Listener	2002
Oracle TCF Server	10021-10029, 15000
Oracle Report Review Agent	1526
Oracle Metric Server and Client	9010, 9020

Infrastructure Layers

Oracle Applications

Database

Application/Forms Server

Web Server

Operating System

Operating System

- Get a good UNIX security expert or book
- Use automated scanning tools (e.g., SATAN)
- Install latest operating system patches
- Limit access to production – no developers
- Check `/etc/hosts.equiv` and `$HOME/.rhosts` files
 - No access from development to production
- No NFS mounts between development and production
- Use different groups for the oracle and applmgr UNIX accounts
 - Makes maintenance more complex, but segregates responsibilities

File System Privileges

- Review the file permissions on all directories
 - Carefully review the following directories –
 - \$APPL_TOP/admin/
 - \$ORACLE_BASE/ows/
 - \$APACHE_TOP/conf/
 - \$APPCSF
 - \$APPLTMP, \$APPLPTMP, \$REPORTSxx_TMP, etc.
 - \$ORACLE_HOME/network/admin/

Oracle Web Server – 11.0 (mandatory)

- Delete all non-essential virtual directories and sample cartridges
 - Delete /ows-bin/ and /ows-adoc/ virtual directories for all non-admin listeners
 - Delete “Get Listener Info” and “Get Environment” sample cartridges
 - Review all virtual directories with setting of “CN” or “CR” – /OA_HTML/bin/ should be the only one
- Turn off directory indexing for all listeners
 - /OA_TEMP/ directory is vulnerable
- Execute AFOAUTHB.pls script in \$FND_TOP
- Change default admin password

Oracle Web Server – 11.0 (advanced)

- Restrict access to specific IP addresses or domain names
- Change OWS user and group to “nobody”
 - Must change file permissions on certain directories
 - More difficult for ports under 1024, setuid problem
- Check for symbolic links in virtual directories
 - Symbolic link to root would give full access
- Use SSL to encrypt reports
 - Create a listener for reports that uses SSL and a second listener without SSL for JAR download and help
- Enable logging for all listeners

Web Server - 11i

- Apache Listener
 - Review virtual directories
 - Check apps.conf configuration file for virtual directories settings
 - Use SSL on all Apache ports
 - Never start Apache listener as root
 - Enable logging for all listeners
- WebDB Listener
 - The Apache Single Listener configuration is preferred since WebDB does not support SSL
 - DAD configuration contains clear-text apps password
 - Check that (AFOAUTHB.pls) has been executed
 - Protect WebDB admin pages

Application/Forms Server

- Make sure Forms message encryption (40-bit) is enabled
 - Check APPL.env file for
FORMSxx_MESSAGE_ENCRYPTION=TRUE
 - 11i - FORMSxx_HTTPS_NEGOTIATE_DOWN=FALSE
 - 11i - SSL can be used as the communication protocol between the client and forms server. This will provide 128-bit encryption – requires Jinitiator 1.1.8.x. Use ConnectMode = HTTPS.
- Enable logging for Forms Listener
 - Capture IP addresses of incoming connections
- Implement SSL for TCF
 - Set Protocol = SSL

Database

- Limit direct access to the Oracle Database
 - Only DBAs and system administrators
 - No Read accounts or extremely limited
- Review all Oracle database accounts
 - Remove all developer and non-product accounts (SCOTT, etc.)
- Change passwords on all Oracle database accounts
 - Review documentation for changing APPS, APPLSYS, APPS_MRC, CTXSYS, and DBSNMP
 - Change all product accounts (GL, AP, etc.) to a random string
 - Not necessary to change APPLSYSPUB account

Database

- Review all Public and Applsypub privileges
 - Check access to all objects including packages and tables against freshly installed instance
 - Concentrate on custom developed objects and schemas
- Verify all directories in utl_file_dir
 - Minimize directories – pl/sql temporary directory required
 - Never use utl_file_dir = *
- SQL*Net
 - Use Oracle Names to limit TNSNAMES.ORA
 - Use Oracle Advanced Networking Option to encrypt SQL*Net
 - Setup Net8 for specific IP addresses

Database Auditing

- Setup database level auditing
 - Move sys.aud\$ from the system tablespace
 - Enable audit in init.ora (audit_trail = db)
 - Truncate sys.aud\$ table periodically
 - Create views on sys.aud\$ for meaning access to data
- Turn on session level auditing
 - Audit all session connections (audit session;)
 - Provides connection and performance information
- Turn on auditing for other critical or sensitive events
 - Audit user changes (audit create user; audit alter user; audit drop user;)

Oracle Apps Limitations

- Account lock-out
 - Session is ended after 3 invalid attempts, but account is not locked out
- Strong passwords (added 11i)
 - Few limitations on passwords before 11.5.2
- Stale accounts
 - Accounts not accessed after x days not locked out
- Login restrictions (network, time of day, etc.)
 - No restrictions for application logons
- Automatic logoff
 - No logoff of inactive accounts after x minutes

Oracle Applications

- Change passwords and disable default Oracle Applications accounts
 - Disable autoinstall, concurrent manager, feeder system, initial setup, standalone batch process, and wizard accounts
 - Change the password for each account to a random string
- Change Sysadmin account password
- Check guest account has no responsibilities
 - Check DBCs in \$FND_TOP/secure to see which user account is used and profile option GUEST_USER_PWD
- Avoid use of default passwords for new users

Oracle Apps Profile Options

- Set the following profile options –
 - Sign-on Password Length (default 5)
 - Set to a minimum of 6
 - 11i - Sign-on Password Hard to Guess – Yes (default No)
 - 11i - Sign-on Password No Reuse – Yes (default No)
 - Sign-on: Notification – Yes (default No)
 - Sign-on: Audit Level – Form (default None)
 - Logs user sign-on, responsibility selection, and forms usage
 - Truncate FND_SIGNON_xxxx tables periodically
 - Utilities: Diagnostics – No
 - Requires APPS password to use Examine function

Applications Auditing

- Applications only stores created_by and last_updated_by
 - History of changes is not maintained
- Audit fnd_profile_option_values tables to quickly identify changes to system profile settings
- Audit critical and sensitive tables
 - Be very selective in auditing due to performance impacts – avoid tables with more than a few inserts or updates per hour
 - Concentrate on auditing tables that have rows which may be updated several times
 - Responsibilities – fnd_responsibility
 - Oracle DB users – fnd_oracle_userid
 - Menus – fnd_menu_entries
 - Request Groups – fnd_request_group_units
 - Audit Logging – fnd_audit_xxxx
 - Alert definitions – alr_xxxx

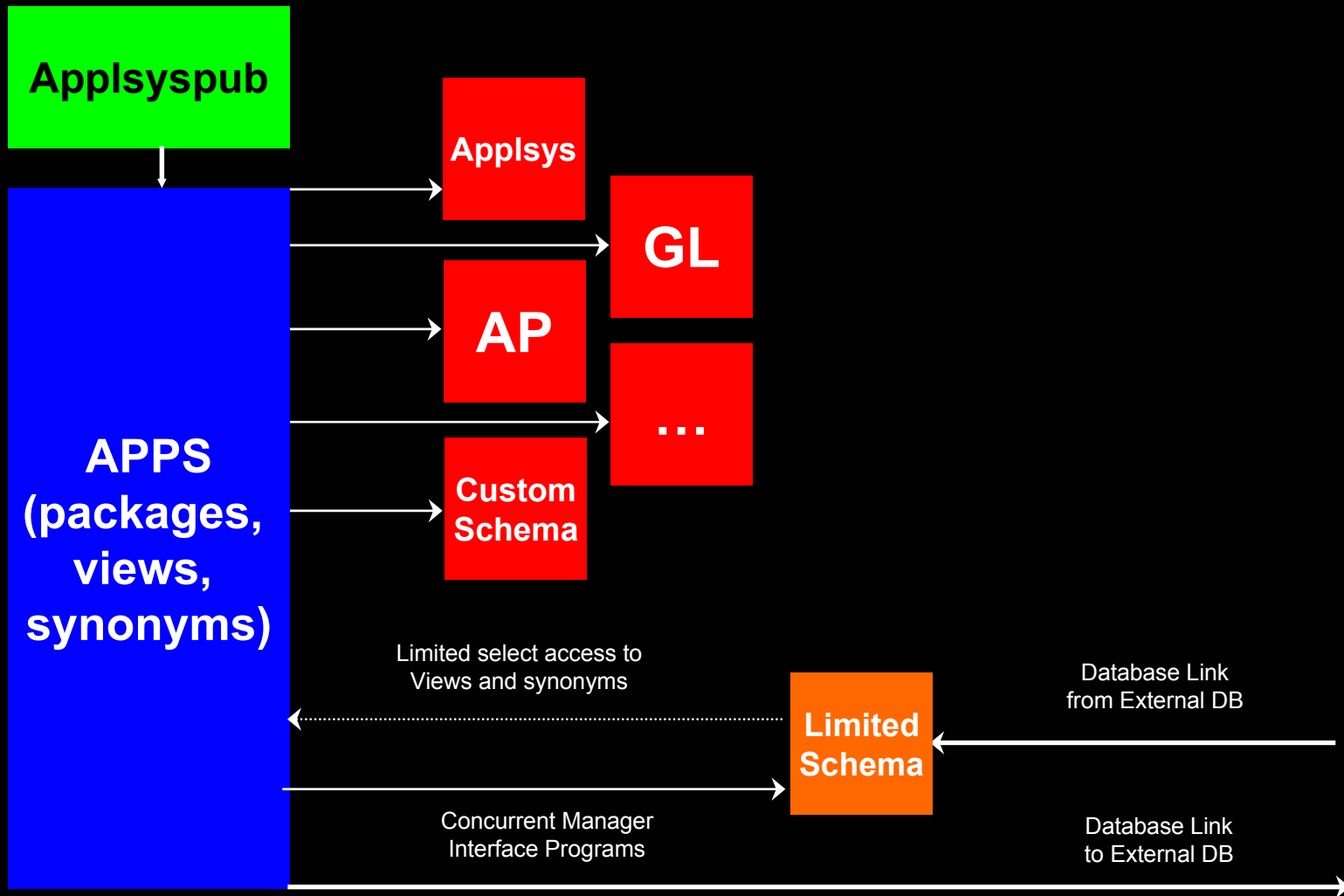
Oracle Alerts

- Use Oracle Alerts to notify system administrators of critical security events
 - Create an alert for the `fnl_unsuccessful_logins` table to send an e-mail in case of multiple invalid logins
 - Must be a periodic alert since user is not logged into Oracle Applications to trigger an event alert
 - Create alerts for other system administration functions
 - Use periodic rather than event alerts for better performance
 - Adding system administrator responsibility to user
 - Identify accounts not accessed for xx days
 - Changes to alerts

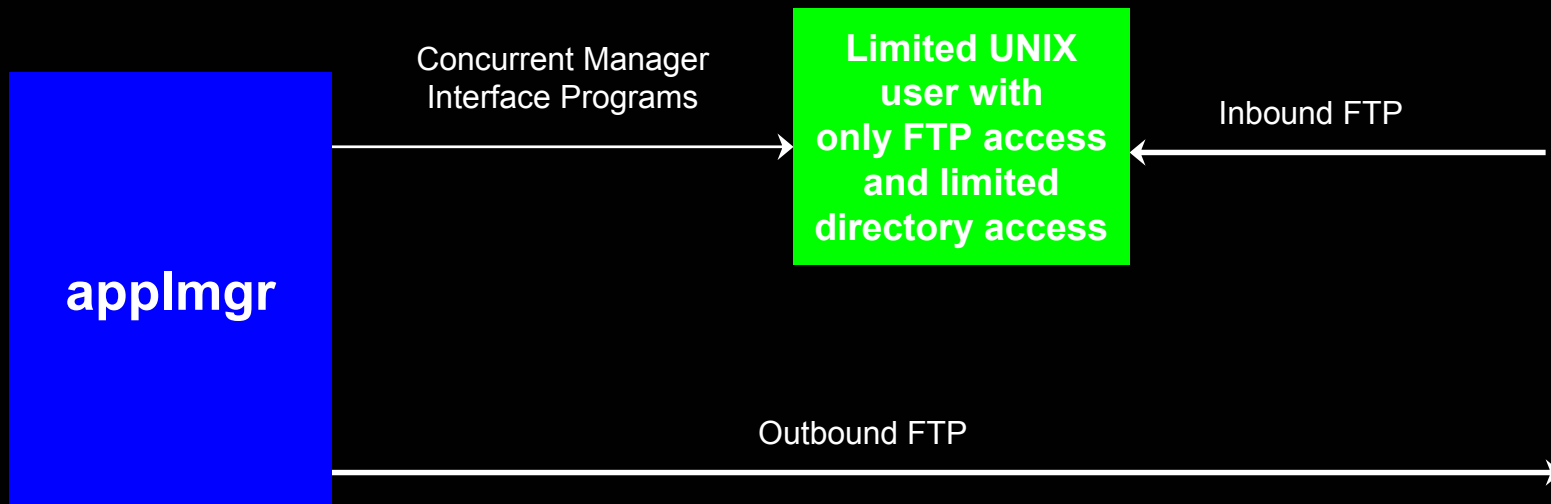
Custom Development

- Change and version control is critical
 - Developers should not be migrating customizations into production
 - Single point of control for all migrations
- Avoid direct access from external systems
 - Database links and ftp should access only extremely limited accounts
 - Compromising of external systems should not compromise Oracle Applications
 - Assume external systems are insecure, but data is valid
- Most security flaws are the result of custom development
 - Invalid grants and poorly designed customizations
 - Multiple methods of development and interfacing
 - Loose access to instances for development

Database Link Interfaces



FTP Interfaces



Development Rules

- Adhere to Oracle Development Standards
 - Deviate only when absolutely necessary
- Only grants on objects should be to apps
 - Grant all on xxx to apps with grant option or use specific grant privileges
- Connect statements should use passed APPS password
- Do not display the apps password
 - Check for apps/apps in output and logfiles
- Use FND_FUNCTION.EXECUTE to open form with security instead of CALL_FORM
- Include created_by and last_updated_by in all custom tables and programs

Integrigy Corporation

Presenter

Stephen Kost
Chief Technology Officer
Integrigy Corporation
stephen.kost@integrigy.com

2052 Lincoln Park West, Suite 1612
Chicago, Illinois 60614
(888) 542-4802
(773) 244-0276 fax

<http://www.integrigy.com>

Copyright © 2002 Integrigy Corporation. All rights reserved.

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