

✓ **INTEGRITY** ✓

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

Securing Oracle Applications – What You Need to Know

Stephen Kost

*Chief Technology Officer
Integrigy Corporation*

Topics

- Introduction
- Oracle Applications
- Oracle Database
- Application Server
- Operating System
- Network
- Integrigy AppSentry

Scope

- Oracle Applications 11i (primarily 11.5.4 – 11.5.9)
- UNIX-based systems
 - Windows Servers have different security issues
- “Average” business
 - Not military, government, or other highly secure sites
- No Internet connected applications
 - Self-Service, iProcurement, etc.
- No CRM (Call Center, Mobile, etc.)
- No Oracle Applications functional security
 - Menus, functions, responsibilities, etc.

Assumptions

- Goal is to improve security, can't make it perfect
- Internal threat is greater than external threat
- Perimeter network is secure
- Security is a cost/benefit proposition
- Undisclosed security holes exist in Oracle Applications
- If someone wants in, they can get in

ERP/CRM Security Problems

- ERP/CRM (Oracle, SAP, PeopleSoft, etc.) packages are massive
 - Millions of lines of code, usually in multiple programming languages
- 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
- Package is often customized or extended
- Testing and security tasks are often late in the application implementation life-cycle

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

Oracle Applications

Database

Application Server

Operating System

Network

Oracle Applications Security Issues

Oracle Applications

Database

Application Server

Operating System

Network

- Complex environment with multiple products and technologies (database, application server, etc.)
- 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
- Too many “Keys to the Kingdom”
 - UNIX – **root, oracle, applmgr**
 - Database – **system, sys, apps, applsys**
 - Applications – any account with **sysadmin** responsibility

- Change passwords and disable unused default Oracle Applications accounts (10-15 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

Password Profile Options

- Signon Password Length
 - Default = “5” characters
 - Recommendation = at least “6” characters

- Signon Password Hard to Guess
 - Default = “No”
 - Recommendation = “Yes”
 - If custom password rules are required, use Signon Password Custom profile option to define a custom validation Java class

- Signon Password No Reuse
 - Default = “0” days – no limits on password reuse
 - Recommendation = at least “180” days

- Signon Password Failure Limit
 - Default = “0” attempts – no lockout
 - Recommendation = “3”
 - Implement alert or custom workflow to notify admin of lockout
 - Available in 11.5.7, FND.E, or Patch 2061872

Security Profile Options

■ Sign-on: Audit Level

- Default = "None"
- Recommendation = "Form"
- Logs user sign-on, responsibility selection, and forms usage
- Use standard Signon Audit reports to view data
- Truncate FND_SIGNON_xxxx tables periodically

■ Sign-on: Notification

- Default = "No"
- Recommendation = "Yes"

■ ICX: Session Timeout

- Default = none
- Recommendation = "30" minutes
- Available in 11.5.7, FND.E or Patch 2012308
- Also set JServ session.timeout in **zone.properties** to equivalent value in seconds

Diagnostics Profile Options

- Utilities: Diagnostics (Forms)
 - Default = “No”
 - Recommendation = “No” at Site Level, “No” for Sysadmin Responsibility
 - Sysadmin Responsibility defaults to “Yes”, even though it may be set to “No” at the Site Level
 - Requires APPS password to use Examine function
 - Usually set to “Yes” during implementation – should be checked

- Hide Diagnostics menu entry (Forms)
 - Default = “No”
 - Recommendation = “Yes” at Site Level, “No” for Sysadmin Responsibility
 - Hides Diagnostics menu

- FND: Diagnostics (Self-Service)
 - Default = “No”
 - Recommendation = “No”
 - Requires APPS password to use Examine function
 - Usually set to “Yes” during development

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
 - Use database triggers instead of Applications AuditTrail
- Audit critical and sensitive tables
 - Be very selective in auditing due to performance impacts

Responsibilities	fnd_responsibility
Oracle DB users	fnd_oracle_userid
Menus	fnd_menu_entries
Audit Logging	fnd_audit_xxxx
Alert definitions	alr_xxxx

- For more detailed information, see “Guide to Auditing in Oracle Applications” at <http://www.integrigy.com/resources.htm>

- Use Oracle Alerts to notify system administrators of critical security events
 - Create an alert for the **fnd_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 an alert if account lockout feature is enabled
 - Create alerts for other system administration functions
 - Use periodic rather than event alerts for better performance
 - Alert when system administrator responsibility is added to a user
 - Weekly or monthly alert to identify accounts not accessed for xx days

Security Alerts

Oracle Applications

Database

Application Server

Operating System

Network

- **Oracle Security Alert #57** – 11.0.x, 11.5.1 – 11.5.8
 - Buffer overflow in **FNDWRR.exe**
- **Oracle Security Alert #56** – 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 **FNDIFS** program
 - Retrieve any file from O/S
- **Oracle Security Alert #44** – 11i FND.C – FND.F
 - **AolSecurityPrivate.class** authentication vulnerability
- **Oracle Security Alert #32** – 11.5.1 – 11.5.6
 - SQL Injection vulnerability in **FND_GFM PL/SQL** Package

Integrigy security alerts are available at <http://www.integrigy.com/resources.htm>

Oracle Applications Patches

Oracle Applications

Database

Application Server

Operating System

Network

- **Patch 2992947** – Updated PL/SQL Package Security
 - Updated list of web-enabled PL/SQL Packages
 - Included in 11.5.9 and FND.G
- **Patch 2077791** – Password Security Enhancement
 - Improved password encryption
 - Included in 11.5.6 and FND.E
- **Patch 1779336** – Enable Server Security
 - Authentication of middle-tier servers
 - Included in 11.5.5 and FND.D
- **Patch 2012308** – Session Timeout Feature
 - Timeout of sessions using new profile option
 - Included in 11.5.7 and FND.E

Server Security Feature

Oracle Applications

Database

Application Server

Operating System

Network

- Provides a trust mechanism for application servers and clients connecting to the database server
 - Prevents rouge applications from connecting
 - Works at the application layer and does not prevent direct SQL*net connections to the database
- Server Security feature is disabled by default
- Implemented in 11.5.5, FND.D, and Patch 1779336
- Three levels of security – OFF, ON, SECURE
 - Always use SECURE
- Carefully test before implementing in Production
 - Especially ADI and Discoverer
- For more information -- System Admin Guide, Appendix G

Database Security Issues

Oracle Applications

Database

Application Server

Operating System

Network

- Database model, init.ora parameters, configuration, and schemas determined by Oracle and should not be changed
 - 150+ 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 security vulnerabilities in Oracle Database and TNS Listener
 - Default TNS Listener configuration (listener.ora) is not secure

Database Security

Oracle Applications

Database

Application Server

Operating System

Network

- Limit direct access to the Oracle Database
 - Only DBAs and system administrators
 - No Read accounts 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
 - Change all product accounts (**GL**, **AP**, etc.) to a random string – use SQL script to generate **FNDCPASS** script
 - Not necessary to change **APPLSYSPUB** account

Database Security

Oracle Applications

Database

Application Server

Operating System

Network

- 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
- Verify all directories in **utl_file_dir**
 - Minimize directories – PL/SQL temporary directory required
 - Never use **utl_file_dir = ***
- Review Oracle security alerts periodically

Database Auditing

Oracle Applications

Database

Application Server

Operating System

Network

- 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;)
 - Audit database links (audit database link; audit public database link;)
 - Audit audit statements (audit system audit;)

Oracle TNS Listener

Oracle Applications

Database

Application Server

Operating System

Network

- Oracle Applications has two listeners
 - Database Home – Database/Extproc Listener
 - 8.0.6 Home – FNDFS/FNDSM Listener
- Set a Listener password
- Turn on logging within the Listener
- Set ADMIN_RESTRICTIONS = ON
- Apply Listener security patches
 - Multiple security vulnerabilities
- Setup valid node checking
 - Restrict listeners to only Application Servers
- For more information, see the “Oracle Database Listener Security Guide” at <http://www.integrigy.com/resources.htm>

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

Oracle Applications

Database

Application Server

Operating System

Network

- 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
 - See the Integrity Security Alert “Internet Connected Applications and Search Engines” at <http://www.integrity.com/resources.htm> for more detailed information.

Application Server – Forms/Reports

- Reports server may disclose the **APPS** password
 - Add “SetEnv REPORTS60_CGINODIAG=Yes” in Apache configuration file (httpd.conf)
 - See the Integrigy Security Alert “Oracle Reports Server APPS Password Disclosure” at <http://www.integrigy.com/resources.htm> for more detailed information
- Setup the Forms Server to use a log file
 - Only mapping between forms session and IP address

Application Server - Modplsql

Oracle Applications
Database
Application Server
Operating System
Network

- 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_/`

- Review file permissions on the following accounts that contain plain-text passwords –
 - iAS_TOP/Apache/modplsql/cfg/wdbsvr.app
 - 8.0.6/reports60/server/CGIcmd.dat
 - FND_TOP/secure/<host_name>_<instance>.dbc
 - APPL_TOP/admin
- Use secure shell (SSH) instead of Telnet and FTP
- Apply latest operating system patches

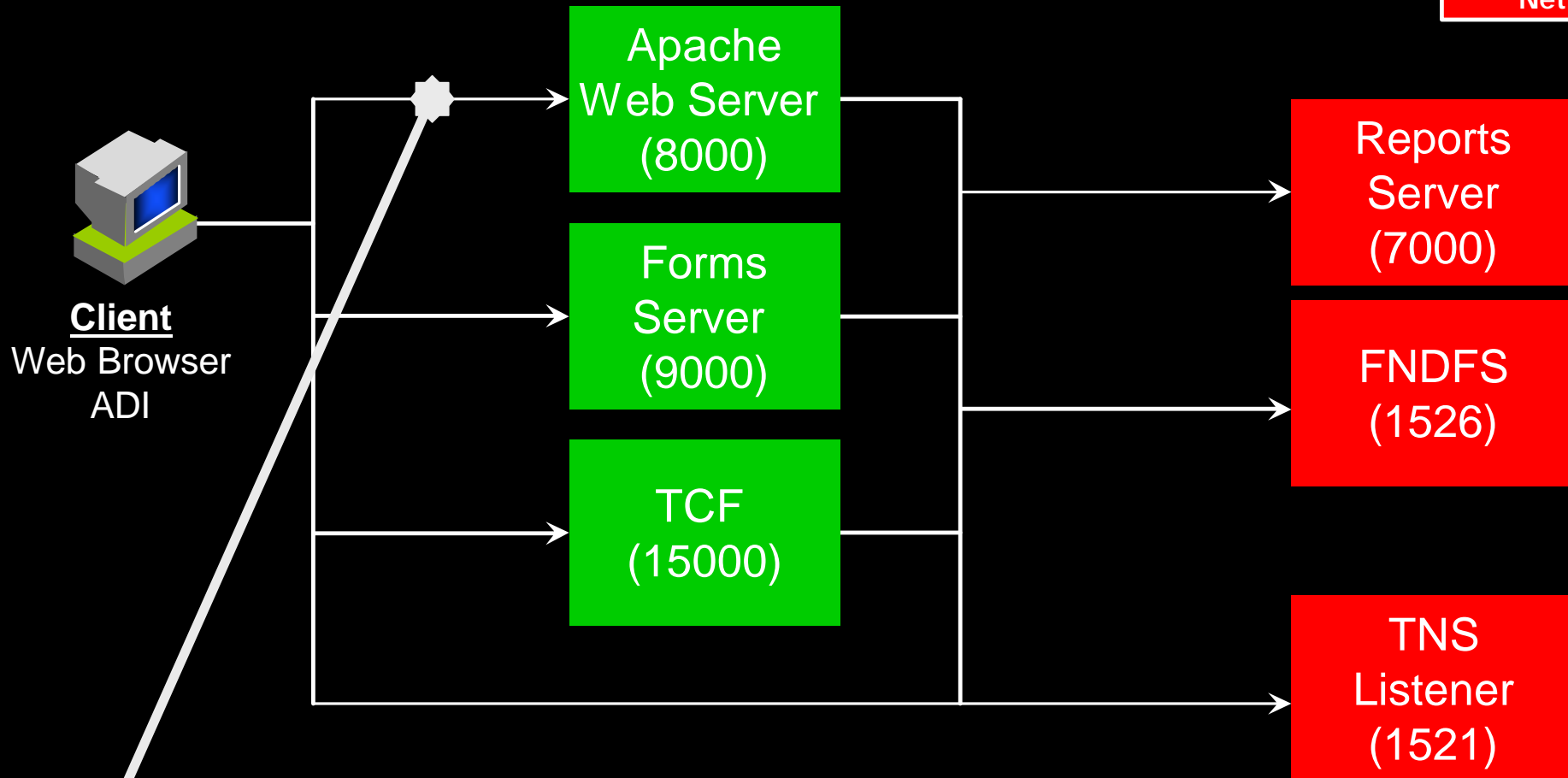
Network Issues

Oracle Applications
Database
Application Server
Operating System
Network

- All network traffic is not encrypted by default
 - Additional complex configuration required
- Multiple types of network traffic
 - Makes firewall configuration difficult
- Many open network ports

Network – Apache

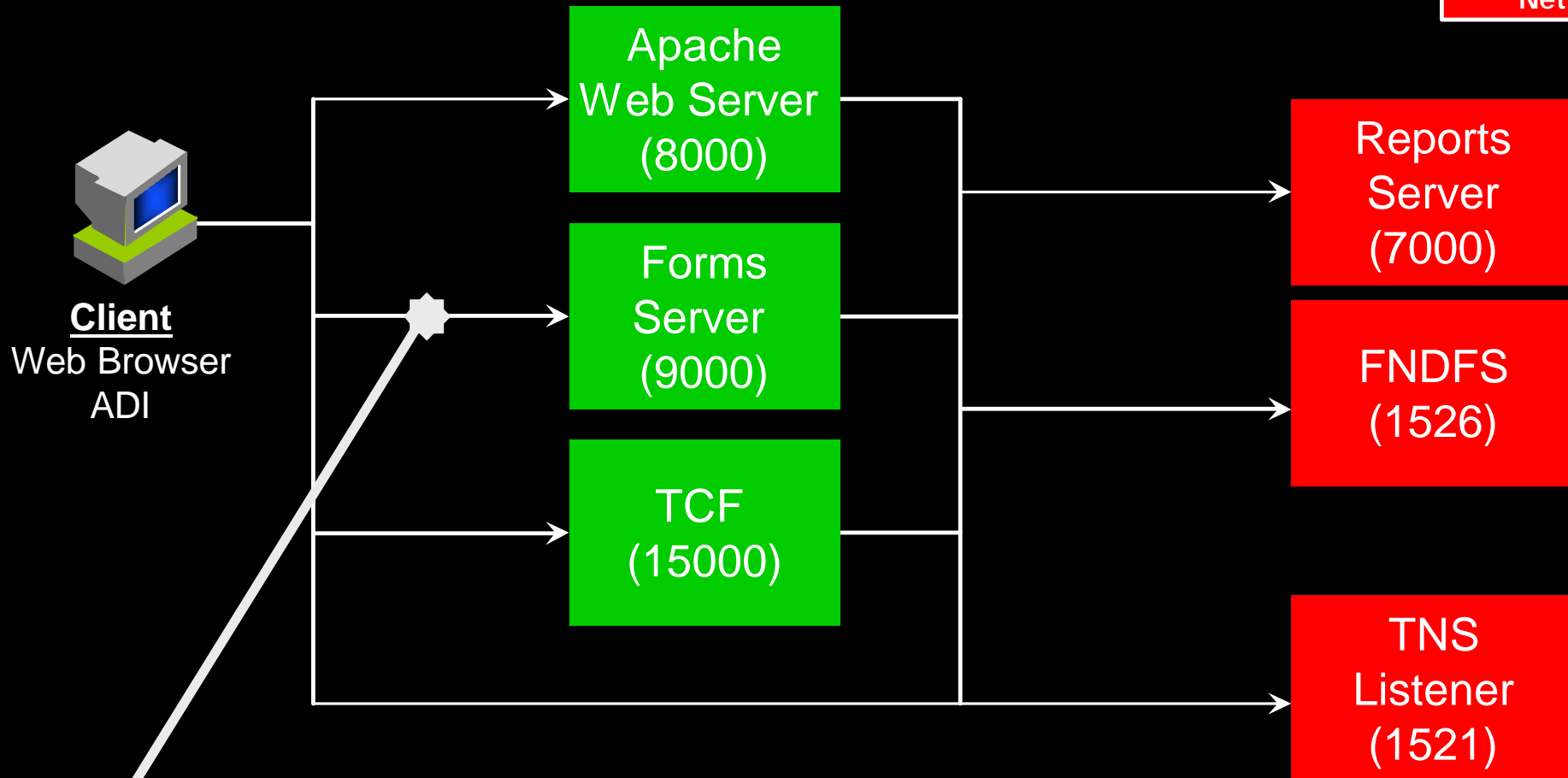
Oracle Applications
Database
Application Server
Operating System
Network



- Default Apache configuration is HTTP – not encrypted
- Password and other sensitive data in Self-Service not encrypted
- To implement SSL, see Metalink Note ID 123718.1

Network – Forms Server

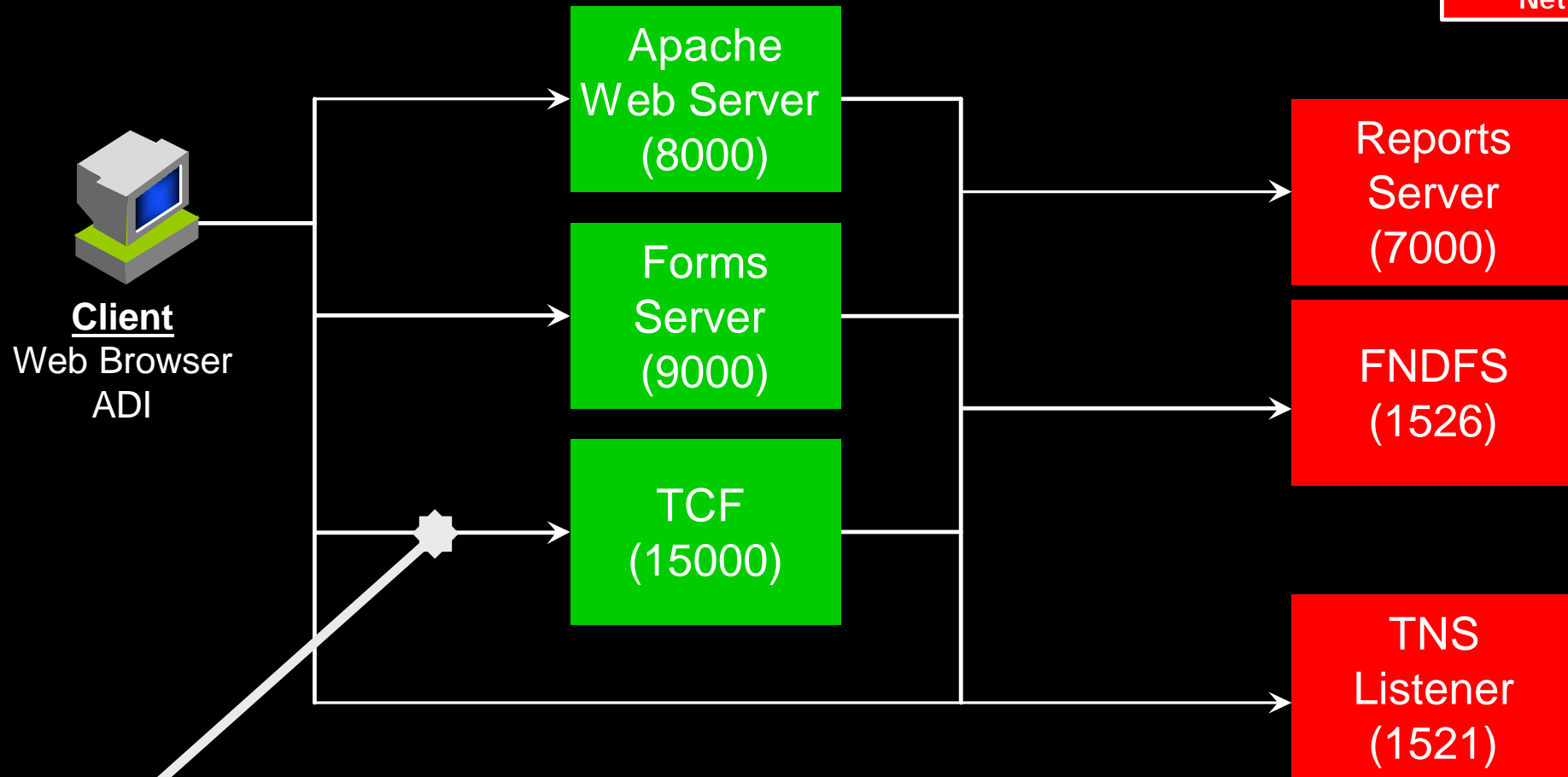
Oracle Applications
Database
Application Server
Operating System
Network



- Forms Server can use Socket (default 40-bit encryption) or HTTPS (SSL)
- Use Socket or Forms Servlet for internally, HTTPS or Servlet for Internet
- To implement SSL, see Metalink Note ID 123718.1

Network – Thin Client Framework

Oracle Applications
Database
Application Server
Operating System
Network



- Default TCF configuration is to use HTTP – not encrypted
- To implement SSL, see Metalink Note ID 123689.1
- Or upgrade TCF to servlet mode, Patch 3034091

- AppSentry for the Oracle E-Business Suite
 - Only security scanner available for Oracle Applications
- AppSentry automates and streamlines the identification of vulnerabilities, security risks, and configuration issues to an extent not previously possible
- Over 300 audits and checks specifically written for Oracle Applications – network, operating system, web server, application server, database, and application

Additional Information

- 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?

Integrigy Corporation

2052 Lincoln Park West, Suite 1301
Chicago, Illinois 60614
(888) 542-4802
(773) 244-0276 fax

<http://www.integrigy.com>

Presenter

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

Copyright © 2003 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