



You vs. The Bad Guys – The Top 10 List For Securing R12

Randy Giefer

Senior Technical Consultant

Solution Beacon

rgiefer@solutionbeacon.com

4948



Copyright © 2011 Solution Beacon, LLC All Rights Reserved
Any other commercial product names herein are trademark, registered
trademarks or service marks of their respective owners.





Objectives

- Provide detailed explanations and mitigations for a prioritized list of ten security improvements.
- Share experiences and knowledge in securing R12
- Increase the attendee's overall Security awareness.



Miscellaneous

- The associated whitepaper for this presentation contains much, much more content than this presentation!
- The most recent version of the whitepaper:
www.solutionbeacon.com/r12securitytop10giefer.pdf
- The author can be reached at:

rgiefer@solutionbeacon.com



Guiding Documents

- Best Practices For Securing Oracle E-Business Suite Release 12 [ID 403537.1]
- Oracle E-Business Suite R12 Configuration in a DMZ [ID 380490.1]
- Oracle® Applications System Administrator's Guide – Security Release 12.1 Part No. E12843-03
- Database Security Guide 11g Release 2 (11.2) Part No. E10574-04



An Approach To Security

Protect.

Detect.

React.



Protect, Detect, React



Securing R12 Top 10 List

Know Your Technology Stack



Know Your Technology Stack

- Sounds Easy
- Need To Know:
 - R12 Technology Stack (not so simple)
 - Other R12 System Components (SOA, BI, etc.)
 - OS
 - Network
- Oracle eSeminar TOI: Oracle E-Business Suite Technology Stack Functional Overview



Know Your Technology Stack

- Constantly Changing

Component	12.0.0	12.0.4	12.1.1
Database	10.2.0.2	10.2.0.3	11.1.0.7
OracleAS 10.1.2 Forms & Reports	10.1.2.0.2	10.1.2.2	10.1.2.3
OracleAS 10.1.3 OC4J	10.1.3.0.0	10.1.3.0.0	10.1.3.4
App Tier Java (JDK)	1.5.0_10	1.5.0_13	1.6.0_10
Desktop Client Java (JRE)	1.5.0_10-erdist	1.5.0_13	1.6.0_u10

- 15 New Technology Stack Enhancements in EBS 12.1.1 - <http://blogs.oracle.com/stevenChan>



Securing R12 Top 10 List

Implement A Secure Architecture



Secure Architecture

- An Architecture is Mandatory
- Three interrelated areas that need analysis:
 - Network Attack Surface
 - Software Attack Surface
 - Human Attack Surface
- Oracle E-Business Suite R12 Configuration in a DMZ, [ID 380490.1]
- Don't be misled by the DMZ reference in the title



Securing R12 Top 10 List

Strictly Control Direct Database Access



Control Direct Database Access

- This control has two main components:
 - A White List of Allowed Hosts
 - Reducing the Number of Allowed Hosts
- Allowed Hosts via sqlnet.ora:
 - tcp.validnode_checking
 - tcp.invited_nodes

```
tcp.validnode_checking = YES
```

```
tcp.invited_nodes = (192.168.1.91)
```



Control Direct Database Access

- Reducing the Number of Allowed Hosts
- Note 277535.1's pertinent statements are:

Oracle recommends that all components requiring direct connection to the E-Business Suite database are deployed on servers rather than on end user desktop machines. The E-Business Suite architecture mostly supports this requirement natively through a three-tier deployment in which end user browser sessions connect to a middle tier of servers running Oracle 9i Application Server. For the few exception cases in which Oracle E-Business Suite components or associated development tools are not directed through Oracle Application Server, it is recommended that they are deployed in a remote server environment using either Windows Server Terminal Services, Citrix or Tarantella.



Securing R12 Top 10 List

Control and Protect “Data In Transit”



Protect “Data In Transit”

- Protecting “Data In Transit”, or “data in the air”, is primarily covered by:
 - Encrypting HTTP Traffic
 - Encrypting Database Traffic
- Encrypt HTTP Traffic:
 - *Enabling SSL in Oracle Applications Release 12 [376700.1]*
- Encrypt Database Traffic:
 - Oracle Advanced Security Option (ASO)



Filter HTTP Traffic

- Application Firewall (URL FW)
- Appendix B of the *Oracle E-Business Suite Release 12 Configuration in a DMZ* [ID 380940] contains the current list of certified R12 products that can be deployed for external use.
- Only implements a “white list”



Filter HTTP Traffic (cont.)

- Need additional attack prevention for:
 - Layer 7 DoS
 - Brute force
 - Cross-site scripting
 - SQL injection
 - Parameter tampering
 - Session highjacking
 - Buffer overflows
 - Cookie manipulation
 - Various encoding attacks
 - Forceful browsing
 - XML bombs/DoS



Securing R12 Top 10 List

Restrict OAS Pages and Prevent Information Disclosure



Restrict OAS Pages

- Protect Administrative Pages

```
<Location "uri-to-protect">  
Order deny,allow  
Deny from all  
Allow from localhost <list of TRUSTED IPs>  
</Location>
```

- Disable Test Pages

```
<Location ~ "^/fcgi-bin/echo.*$">  
Order deny,allow  
Deny from all  
</Location>
```



Prevent OAS Information Disclosure

- Create your own “Safe” error pages

```
< ErrorDocument 500 /my_custom_500_error.htm
```

- Disable OAS Banner Information

```
ServerSignature OFF  
ServerTokens Prod
```

Suppresses trailing footer lines, OS, virtual hosts, and version info



Securing R12 Top 10 List

Mitigate Known Vulnerabilities



Mitigate Known Vulnerabilities

- Hackers Reverse Engineer CPU Patches
- Patch Current!
- Critical Patch Updates and Security Alerts
 - <http://www.oracle.com/technology/deploy/security/alerts.htm>
 - Security Alerts and Critical Patch Updates - Frequently Asked Questions [ID 360470.1]
- Oracle's security alert notification system via:
<http://www.oracle.com/technology/deploy/security/securityemail.html>



Mitigate Known Vulnerabilities

- Critical Patch Update Implementation Best Practices:
http://www.oracle.com/technology/deploy/security/pdf/cpu_whitepaper.pdf
- The next four CPU dates are:
 - 19 April 2011
 - 19 July 2011
 - 18 October 2011
 - 17 January 2012
- The Bad Guys Know These Dates Too!
- Plan for it. Prepare. Protect yourself.



Securing R12 Top 10 List

Harden R12 Profiles and Passwords



Harden EBS R12 Using Profile Options

- Secure Configuration of E-Business Suite Profiles [946372.1]
 - FND: Diagnostics -> NO
 - FND Validation Level -> ERROR
 - FND Function Validation Level ->ERROR
 - Framework Validation Level -> ERROR
 - Restrict Text Input -> Yes



Harden R12 App Passwords and Password Controls

Profile	Default	Recommendation
Signon Password Failure Limit	None	3 (attempts)
Signon Password Hard to Guess	No	Yes
Signon Password Length	5	8 (characters)
Signon Password No Reuse	None	180 (days)
Signon Password Custom	None	See Note Below
Signon Password Case	None ^{*1}	Sensitive



Harden R12 App Passwords and Password Controls

Account	Product / Purpose	Change	Disable
AME_INVALID_APPROVER	AME WF migration 11.5.9 to 11.5.10	Y	Y
ANONYMOUS	FND/AOL – Anonymous for non-logged users	Y	Y
APPSMGR	Routine maintenance via concurrent requests	Y	Y
ASGADM	Mobile gateway related products	Y	Ya
ASGUEST	Sales Application guest user	Y	Yb
AUTOINSTALL	AD	Y	Y
CONCURRENT MANAGER	FND/AOL: Concurrent Manager	Y	Y
FEEDER SYSTEM	AD – Supports data from feeder system	Y	Y
GUEST	Guest application user	Y	N



Securing R12 Top 10 List

Harden the End Point



Harden the End Point

- Client Browser
- Recommended Browsers for Oracle E-Business Suite Release 12 [ID 389422.1]
 - Internet Explorer for Windows Users
 - Firefox for Windows Users
 - Safari for Mac Users
- Don't be misled by the title - addresses more than just 'recommended browsers'



Harden the End Point

- Don't be misled by the title - addresses more than just 'recommended browsers', such as settings that deal with:
 - Security Zones
 - JRE Plug-ins
 - Use of Excel with ADI
 - Autocomplete
 - Keep Alive
 - Certificates
 - Cross Site Scripting Errors
 - Attachments
 - Exporting Data



Securing R12 Top 10 List

Implement R12 Functional Security



R12 Functional Security - MOAC

- MOAC: Multi-Org Access Control
- Role based access to Operating Units (OU)
- Security Profiles for data security
 - MO: Security Profile
 - List of operating units for a responsibility
 - Defined in HR
- OU field on UI
 - all transactions
 - setup data specific to OU, like transaction type



R12 Functional Security - MOAC

- Enhanced Multi-Org Reporting and Processing
 - Ledger/Ledger Set parameter on accounting reports and processes
 - OU parameter on other standard reports and processes



R12 Func Security – GL Access Sets

- Data Access Sets
 - Grant and tailor access to Ledgers and Balancing Segment Values (i.e. Companies, Stores, Branches, etc.)
- Definition Access Sets – separate from data security
 - Share, restrict definitions; privileges to view, modify, etc.



Protect, Detect, React



Securing R12 Top 10 List

Enable and Monitor Logs



Enable Mid-Tier Logs

- How to enable Apache, OC4J and OPMN logging in Oracle Applications R12 [ID 419839.1]

Log	Level Description
alert	Action must be taken
crit	Critical conditions
debug	Debug level messages
emerg	Emergencies, system is not useable
error	Error conditions
info	Information
notice	Normal but significant condition
warn	Warning conditions



Monitor Mid-Tier Logs

- The Apache log files are written to:
`$LOG_HOME/ora/10.1.3/Apache`
- The logs consist of:
 - Access Log (CustomLog) - the filename format
`access_log.<unique id>`
 - Error Log (ErrorLog) - the filename format is:
`error_log.<unique id>`



Monitor Mid-Tier Logs

- The following logs can also provide important event information:

`$LOG_HOME/ora/10.1.3/Apache/mod_rewrite.log`

`$LOG_HOME/ora/10.1.3/Apache/sec_audit.log`

`$LOG_HOME/ora/10.1.3/Apache/sec_debug.log`



Enable Listener Log

- To enable Listener logging, set the following parameters in \$TNS_ADMIN/listener.ora:

```
LOG_STATUS = ON  
LOG_DIRECTORY_$(ORACLE_SID) =  
$TNS_ADMIN  
LOG_FILE_$(ORACLE_SID) = $(ORACLE_SID)
```



Enable DB Auditing

AUDIT_TRAIL settings

Parameter Value	Meaning
DB	Enables database auditing and directs all audit records to the database audit trail (SYS.AUD\$), except for records that are always written to the operating system audit trail
DB_EXTENDED	Does all actions of AUDIT_TRAIL=DB and also populates the SQL bind and SQL text columns of the SYS.AUD\$ table
XML	Enables database auditing and directs all audit records in XML format to an operating system file
XML_EXTENDED	Does all actions of AUDIT_TRAIL=XML, adding the SQL bind and SQL text columns
OS	Enables database auditing and directs all audit records to an operating system file



Enable R12 Auditing

Profile Option Name	Description	Recommend Value
AUDITTRAIL:ACTIVATE	Enable R12 Auditing	Yes
SIGNONAUDIT:LEVEL	Set at site-level to track actions starting when the user logs on.	Form

SIGNONAUDIT:LEVEL Possible Values:

None

User

Responsibility

Form



Protect, Detect, React



Incident Response

- Final Component of the P-D-R Trinity; React.
- P³ (Prepare, Plan, Practice)
 - Prepare
 - Need Inventories
 - Need Information At Your Fingertips
 - Plan
 - Need to plan for what to do in various scenarios
 - Practice
 - Practice and Observe



TOP 10 Review

- Know Your Technology Stack
- Implement a Secure, Overall Architecture
- Strictly Control Direct Database Access
- Control and Protect “Data In Transit”
- Restrict OAS Pages and Prevent Information Disclosure
- Mitigate Known Vulnerabilities
- Harden EBS R12 Profiles and Passwords
- Harden the End Point
- Implement R12 Functional Security
- Enable and Monitor Logs



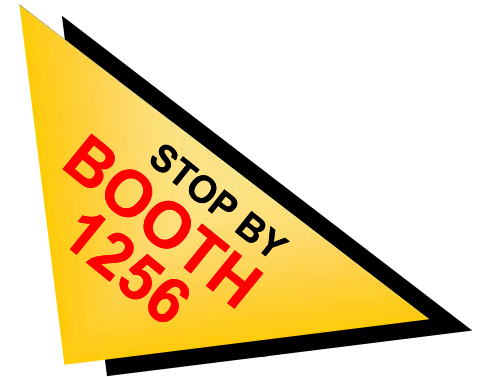
Conclusion

- Don't neglect other security controls and best practice recommendations – they are important!
- Security does not “just happen”
- Security is a continual process
- Security is no longer an option



Ranked R12 Scorecard Technical Consultation

- Get Your Technical Scorecard Today
 - Identify areas of risk
 - Suggest cost saving opportunities
 - Provide checklist of next steps
- See Your Technical Assessment Options
 - Upgrade readiness, customization reduction, Hardware/Architecture, Workflow, Health Check, Security
 - All provide technical recommendations, best practices and performance/efficiency improvements and ROI



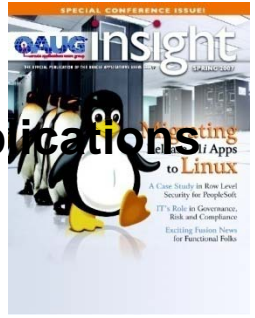
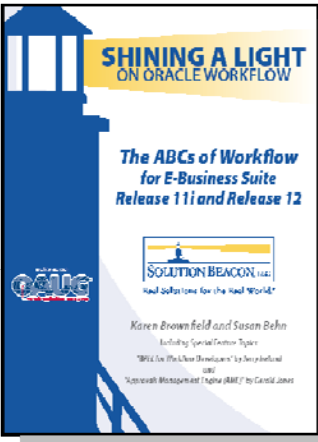
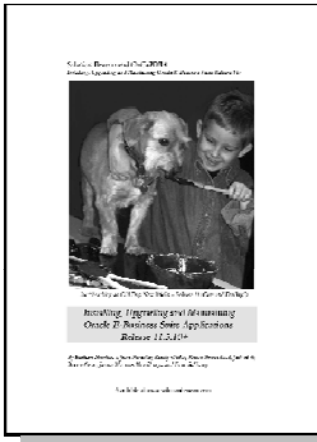
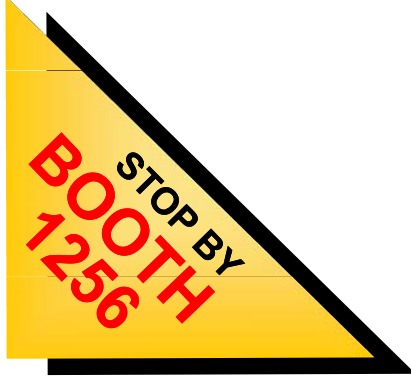
Time is money. A Technical Assessment can identify how to reduce technical expenses for all future upgrades.



Assessments	Implementations
<ul style="list-style-type: none"> • Strategic business assessments & ROI • Functional assessments • Technical assessments • IT roadmap planning • Acquisition integration • Software selection • Upgrade readiness 	<ul style="list-style-type: none"> • ERP upgrades • ERP implementations • ERP migration and consolidation • Oracle Fusion Middleware - SOA • Develop industry specific front-end modules • Custom development • International dependencies and multi-org
Optimizations	Support Services
<ul style="list-style-type: none"> • Business process re-engineering • Functional optimization • Technical optimization • System architecture optimization • Database tuning and optimization 	<ul style="list-style-type: none"> • Functional and technical support • Focused knowledge transfer • Remote DBA support • Oracle instance hosting



Published Authority on Oracle



National Publications





Questions?



Copyright © 2011 Solution Beacon, LLC All Rights Reserved
Any other commercial product names herein are trademark, registered
trademarks or service marks of their respective owners.

