11i Application Security – How to Achieve it With Minimal Bank Balance $$$ - The Poor Man's Way!!!

Khalid Hameed
Oracle Applications DBA

- Information Technology Experience 10 Years
- Applications DBA for over 8 years
- Applications DBA at the City for almost 5 Years
- Khalid.Hameed@stpete.org

City of St. Petersburg Overview

- Residents: 250,000
- Employees: 3,600
- Oracle Environment
  - Oracle Applications 11.5.10.2
  - Oracle 10gR2
  - Sun Solaris 9, 10

AGENDA

- Why Security?
- Role of DBA
- Levels of Security
- Resources
- Q & A

Why Security?

- **Business continuity**
  - **Availability**
- **Legal obligations**
  - **Confidentiality**
- **Loss of reputation**
  - **Integrity**

Role of DBA

- First line of defense against security threats
- Act as a Security Guard
- Develop partnership with auditors and security officers
- Take a proactive role versus reactive

Levels of Security

- Database Security
- Application (Apps) Security
- Operating System (O/S)
  - Oracle Application Security at the System Level
  - Network Security
  - Local Server Security

Database Security

- Change default passwords
  - System, Sys, Scott, Outln etc.
  - Patch 4926128 - Oracle Default Password Scanner
  - Force password complexity (*Note: 114930.1*)
- Disable accounts not in use
  - dbsnmp, mdsys, ctxsys etc. (Note: 160861.1)

Database Security (cont'd)

- Limit access to dictionary tables
  - 07_DICTIONARY_ACCESSIBILITY=FALSE (Note:153510.1)
- Limit file system access within PL/SQL
  - Avoid UTL_FILE_DIR = *

Database Security (cont'd)

- Ensure no user has ALTER SESSION and ALTER SYSTEM privileges
- Users should only login to prod using read-only account
- Prevent users from sharing account ID's

Database Security (cont'd)

- Check use of system tablespace by default and SYSTEM users.
- Turn Audit on sensitive tables and views. (Fine grain auditing)
  - Session, User, Database link etc.
- Audit failures on critical objects
  - Updates and Deletes etc.

Database Security (cont'd)

- Backup and recovery procedures
- Document recovery procedures
- Schedule cold backups
- Ensure the database is in archive log mode
- Validate the backup media regularly on-site and off-site
- Store backup media off-site

Apps Security

- Change passwords for seeded application user accounts
  - Sysadmin, Guest
- Use FNDCPASS utility to change apps/applsys passwords
- Tighten up log on security
  - SIGNON_PASSWORD_LENGTH = 8
  - SIGNON_PASSWORD_HARD_TO_GUESS = Yes
  - SIGNON_PASSWORD_NO_REUSE = 180
  - ICX_SESSION_TIMEOUT = 30

Apps Security (cont'd)

- Oracle Critical Patch Update
  - Note: 432865.1
- 11i.ATG_PF.H.Delta.6 patch level
  - Released twice a year
- Encrypting Concurrent Programs
- Use ssl (https) between browser and web server
  - "11i: A Guide to Understanding and Implementing SSL for Oracle Applications"

Apps Security (cont'd)

- Review users with administrative responsibilities
- Restrict Responsibilities by web trust level using "NODE_TRUST_LEVEL" profile (Note 287176.1)
  - administrative
  - normal
  - external

Apps Security (cont'd)

- Audit by using profile option "Sign-On:Audit Level“
  - None, User, Responsibility and Form
- AUDIT REPORTS
  - Signon Audit Forms
  - Signon Audit Concurrent Requests
  - Signon Audit Responsibilities
  - Signon Audit Unsuccessful Logins
  - Signon Audit Users
- Set “AuditTrail:Activate” to Yes/No

Apps Security (cont'd)

- Purge the audit records on a regular basis
  - FND_LOGIN_RESP_FORMS
  - FND_LOGIN_RESPONSIBILITIES
  - FND_LOGINS
  - FND_UNSUCCESSFUL_LOGINS
- Metalink Note 60828.1 – Overview of Oracle Applications AuditTrails
- Metalink Note 69660.1 – Understanding Data Auditing in Oracle Application Tables

Operating System (O/S)

- An attacker should find a very unfriendly environment – Difficult to break into and/or use to attack other systems.
- Application system accounts should be distinct and separate from individual login accounts
  - DBA
    - No root access
    - Uses SU command to become application account
      - (su – appltest)
  - Developers
    - No Direct Logins to Production Instances
    - If Read-only access is required, use SAMBA, etc.

O/S Security (cont'd)

- Check environment variables for usernames and password (env | grep <password>)
- Audit the machine for scripts containing usernames and passwords
- Audit client machines for configuration files containing usernames and passwords
- Beware of the following directories. The apps password sometimes lurks in files there:
  - /u0/oracle/<instance>/appl/admin
  - /u0/oracle/<instance>/ora
  - /u0/oracle/<instance>/db/10.2.0.2/appsutil

O/S Security (cont'd)

- Use Secure Protocols for Administration
  - ssh instead of telnet
  - scp, sftp instead of ftp
  - Remove the infamous remote rcp protocols
    - rlogin, rsh, rexec
- Disable Unused Network Services
  - Echo, discard, daytime, chargen, talk, wall, rquota, comsat, finger, uucp, ftp, and especially telnet
- Disable unused accounts
- Enforce strong passwords for authentication

O/S Security (cont'd)

- Disable Trust Relations with other systems
  - /.rhosts
  - /$HOME/.rhosts
  - /etc/hosts.equiv
- Firewalls Are Essential
  - The First Line of Defense
  - Listener Port 1521 should NOT be accessible from the Internet
- Valid Node Checking
  - $ORACLE_HOME/network/admin/sqlnet.ora
    - tcp.valid_checking = YES
    - tcp.invited_nodes = (10.1.1.2, hostname)

O/S Security (cont'd)

- Keep up to date with system security patches
- Restrict Access to Servers
  - Physical Security
  - Authentication
    - Root Access only to Sys Admins
    - DBAs: SUDO access for specific rootly powers
- Set Correct File Permissions
  - Minimize rw-rw-rw- files
  - Minimize suid/sgid files
- Platform Specific Hardening Suites
  - JASS for Solaris

O/S Security (cont'd)

- Location of temp directories TMP_DIR, TMPDIR and TEMP
- Check permissions of the datafiles
- Check trace file permissions
- Check for remote data access files (RDA)

O/S Security (cont'd)

- Clean all logs after cloning and running adautoconfig.sh
  - Remove Credentials from a Cloned instance (Note: 419475.1)
- Make sure all history files cleared
- Protect trace files (password and sensitive data)

O/S Security (cont'd)

- The fewer people with root access, the easier it is to track changes.

- Doing a "ps -ef | grep sqlplus" on a command line shows password
  - sqlplus apps/password@test
  - sqlplus apps@test

Resources

- http://metalink.oracle.com
  - Best Practices for Securing Oracle E-Business Suite
  - Oracle E-Business Suite 11i Configuration in a DMZ
  - Encrypting EBS 11i Network Traffic using Advanced Security Option / Advanced Networking
- http://www.integrigy.com
  - “Guide to Auditing in Oracle Applications”, Integrigy Corporation
- http://www.petefinnigan.com
  - “Oracle Security - Step by Step”, Pete Finnigan

Resources (cont'd)

- http://www.ioug.org
- http://www.oaug.org

Thank You !