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

Khalid Hameed
City of St Petersburg

Introduction - The intent of this paper is to give an overview of why and how to protect company data and how to accomplish it easily. At the same time, these measures will reduce money spent on third party tools. Although sometimes overlooked, there is a wealth of free and easy to find information on Oracle Application security that should be reviewed before determining what is needed in third party tools. Also, the role of the DBA and System Administrator will be detailed along with the different levels of security.

Why Security? – There are any numbers of reasons that can answer this question, but this paper will cover only a few of the most important reasons for maintaining an effective level of security. First, there is business continuity and making sure that the system is available to users. Second, there are legal obligations to consider. The user community or client needs to know that their information will be kept confidential at all times. If proper security measures are not taken, and there is a break in business continuity or a loss of confidentiality, a company then risks the loss of its reputation and integrity.

Role of the DBA/System Administrator – The role of the DBA and System Administrator is to act as the first line of defense against security threats to the database. With the increase of threats against databases, the role of the DBA is changing. In the past, DBA's were only responsible for backup and recovery, tuning databases, and making sure the database was available to users, etc. But now, the role has expanded to make sure no undesirables try to hack into the system and steal company information. The DBA acts as a security guard against undesirables. In order to achieve this, the DBA needs to have a partnership with auditors and security officers within their company to work together. The DBA needs to take a proactive role versus a reactive role to make sure the environment is safe.

Database Security – It is necessary to change default passwords when installing new databases because it comes with a large number of default user accounts with known passwords. Make sure to change default password such as System Scott, Outln, etc. Also, if an individual has recently joined a company or the database has been installed a longtime ago and one is unsure if the default passwords have been changed, patch 4926128 can be applied. When this database patch is applied in the database it will scan through all the databases and give a report about all the default users with default passwords, if there are any. Also, make sure to disable accounts that are not currently in use in the database (Note: 160861.1). Finally, when setting up passwords, make sure to enforce password complexity. This means the password should be complex enough that hackers cannot hack it, but not so complex that it cannot be remembered unless it is written on a piece of paper.

It is especially important in financial and human resources databases that have sensitive information to allow limited access available to users and this only when the job or responsibility permits. In a bigger organization, it is hard to keep track of how many and who has access to critical information and what it is being used for. In such cases, one can turn audit on sensitive tables on user sessions database links, etc. One can audit statements like updates and deletes, etc. Finally, it is important to run reports against audit tables periodically to find or look for any red flags.

At the City of St Petersburg, there are multiple layers of backup security set up to make sure that in case of any failure we can easily recover and restore and provide our users with a continuous flow of data. Part of that process is making sure that we have all the necessary backup and recovery procedures in place and all the relevant documents are available in case the administration group is not available onsite. In that case, anyone can pick up the documents and following the steps in them, have our system up and running in no time. We schedule cold backups (full backups) every weekend. Also, all of our critical mission databases are in archive log mode. That means the City of St Petersburg can recover without the loss of data at any

point in time. We validate our entire databases whether they are cold or hot backups to make sure they are in good working condition and nothing is corrupt. Finally, the City of St Petersburg stores backup media on site as well as offsite and twice a year we do disaster recovery tests onsite as well as offsite.

Application Security – Oracle applications with all of its complexity has its own challenges to maintain security. Just as any other security, we have to be aware of the balance between security and ease of use for users. Oracle applications right out of the box does not provide any security. This is a process one has to continually work on after the initial installation and it needs to be secure according to an organization's business model or requirements. Just to be aware, the business model of one company might not serve the purpose for another organization. However, at a minimum it can give a road map to customize it according to the needs of differing companies.

At the City of St Petersburg, instead of buying third party tools, we are using Oracle's methodology to secure our application and utilizing what is already available free of cost. When installing fresh Oracle Applications, we make sure to change passwords for seeded application user accounts such as sys admin and guest, etc. It is also important to tighten up security by using different security profiles provided by Oracle Applications, such as SIGNON_PASSWORD_ LENGTH to eight characters, etc. It is important to keep updated on quarterly critical patch updates. Concurrent programs should be encrypted. Set up audits on users with administrative responsibilities. Oracle provides numerous reports that one can run to audit different sections of the application such as forms, concurrent requests, and unsuccessful logins. Finally, further security of Oracle applications can be done by following Oracle note "Best Practices for Securing E-Business Suite" (Note number: 189367.1).

Operating System Security (O/S Security) - In the realm of Oracle Application Security at the System Level, any attacker should find the UNIX system to be a very unfriendly environment, one that is difficult to break into and/or use to attack other systems. At the crux of this, are having the application system accounts to be distinct and separate from the individual login accounts.

For the DBA's, there should be no root access. They also should not log in directly to the application system accounts ora* and appl*. Instead, the su command should be used to effectively become the application account. Care should be taken to inherit the environment correctly.

As for the application developers, they should have no direct logins to the production instances, even with their own personal accounts. If read-only access is required, use a tool like SAMBA to allow browsing of select directories. For example, if the developers are given read-only access to /u0/oracle/prod, be aware that the APPS password may lurk hidden deep in the directory structure.

The APPS password needs to be kept safe. There should be an audit done to mitigate its exposure. First, check the environment variables for usernames and passwords (env | grep <password>). Second, audit the machine for scripts containing usernames and passwords. Third, audit the client machines for configuration files containing usernames and passwords.

Network Security for Oracle Applications is also an area that must be addressed. Most of these "hardening" steps are performed to enhance general server security. However, they are noted here for convenience.

First and foremost, use a secure protocol for administration. SSH is the tool of choice. Use this instead of telnet to access the servers on the command line. In fact, the telnetd daemon should be disabled outright. The tool PuTTY is commonly used for an ssh client. Also, for copying files to and from the server, use a protocol like scp or sftp instead of FTP. FTP, like telnet, does all its communication in plain-text making it extremely easy to see both ftp payloads and login passwords.

Next, remove the infamous remote rcp protocols like rlogin, rsh, and rexec. SSH takes care of these roles now. In addition, remove/disable unused network services. A list of candidates for disabling, includes, but is not limited to: echo, discard, daytime, chargen, talk, wall, rquota, comsat, finger, uucp, ftp, and especially telnet. These services are defined in the /etc/services file as specific names and port numbers. Note that in Solaris 10, disabling them cannot usually be done with the traditional /etc/inetd.conf file. SMF has to be used in Solaris 10.

Accounts also play a role in network security of Oracle Applications. It is recommended to disable unused accounts, lock system accounts that do not have direct login use, and enforce strong passwords for authentication.

Trust relationships with other systems can be a hidden problem which needs to be secured. These are configured in files such as /.rhosts, /$HOME/.rhosts, and /etc/hosts.equiv. These trust relationships were used to make servers "equivalent" to each other by granting permission of other servers to execute remote commands with no authentication. In today's age, this antiquated method should not be used. Note that having a "+" sign in any of these files, permits "any" machine to execute commands remotely. The Plus is a very bad sign in these files.

Firewalls are essentials. This is not really in the realm of the DBA or developer, but there is a need to specify to your networking team the needs of the application. For example, listener Port 1521 should NOT be accessible from the Internet.

There are other networking configurations which we are exploring. One of them is Valid Node Checking. This is set in the $ORACLE_HOME/network/admin/sqlnet.ora file by setting:
tcp.valid_checking = YES
tcp.invited_nodes = (10.1.1.2, hostname)

The third point in Oracle Application Security is that the local server itself should be secured. One should keep up to date with system security patches. New threats are surfacing all the time and it is important to keep abreast of the latest security developments. Secondly, physical security of the server is important. This includes a secure environment with respect to restricting personnel access but also stable power, cooling, etc.

As mentioned earlier, authentication is a primary tool for security of your server. System Administrators should have root access only. The root password (and the APPS passwords for that matter), should be kept in a safe location in the event of an emergency. The DBA's may be granted specific rootly powers using a tool like SUDO. (http://www.sunfreeware.com) SUDO allows the System Administrator to delegate any command to be run as another user being duly authenticated by the real user's password. Thus, a database startup/shutdown script that needs to be run as root can be run as the DBA's user without having the root password known by the DBA's.

One of the greatest challenges in the UNIX environment running Oracle Applications is setting correct file permissions. The number of files with a chmod of 666 or directories with a chmod of 777 should be minimized. This can be done with judicious use of secondary groups.

Conclusion – By following the steps outlined above, an organization can find a number of cost effective ways to enhance their security.

References and Resources:

Jim Schwonek is the Unix Administrator at the City of St Petersburg and he was helpful in providing the information that can be found in the Operating Systems Security portion of this paper.

http://metalink.oracle.com: On this site the following articles can be helpful:
"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.integrity.com:
"Guide to Auditing in Oracle Applications," Integrigy Corporation.

http://www.petefinnigan.com
"Oracle Security – Step by Step," Pete Finnigan.

http://www.ioug.org

http://www.oaug.org