# Security Principles in ERP Systems

**Cosmin PASCU**
*IT&C Security Master*
*Department of Economic Informatics and Cybernetics*
*The Bucharest University of Economic Studies*
*ROMANIA*
cosmin.pascu@gmail.com

*Abstract:* Enterprise Resource Planning systems are a critical component nowadays of any private company or public institution. Because of their complexity and their importance to all the core functions of an organization, security represents a major concern that's often overlooked besides the standard set-up. In this paper I will explain the architecture of Oracle E-Business Suite, one of the most widely spread ERP solutions, its security problems and an approach to solving them, hardening and customizing an Oracle E-Business Suite Application

*Key-Words: ERP, Oracle E-Business Suite, security, database, hardening, three-tier architecture*

## 1. Introduction

An ERP system is an integrated information system that automates business workflows throughout the enterprise and supports operations in key departments such as accounting, budgeting, material resource planning, supply chain management, human capital management, sales and marketing, customer relationship management etc.

Oracle E-Business Suite is a collection of integrated enterprise software applications which allows private and public organizations to efficiently manage business processes and workflows.

The role of Enterprise Resource Planning systems is to aggregate and integrate data from the entire organization while delivering the technological platform for automating and simplifying business workflows.
ERP systems usually replace multiple legacy applications, while integrating the information from multiple sources into a single source of truth and making it available in real time for the company's users and partners.

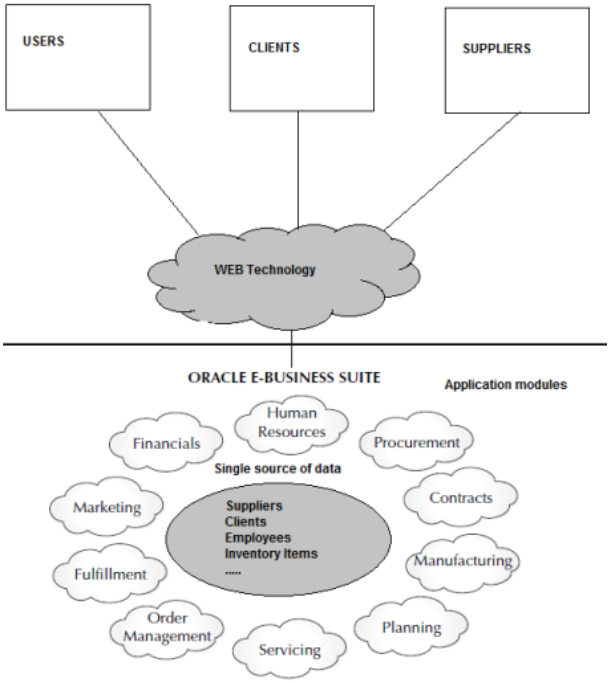


*Figure 1. Shared data model and web architecture*

## 2. ERP Systems Security Challenges

While ERP systems are developed taking in consideration the best practices and the common business processes to most organizations, each implementation is faced with unique requests that cannot always be resolved using the applications setup and configuration options, leaving

ISSN 2067 – 4074

the ERP implementer to search for alternative solutions such as personalizations, extensions, and customizations of new or existing applications.
Because of the critical nature of these systems, the value and confidentiality of the data stored and the impact throughout the enterprise together with laborious implementations that almost always include lots of customizations of the standard solutions, the security of these systems becomes a real problem to the IT administrators.
The most often encountered risks for Oracle E-Business Suite implementations are the following, in order of importance:

1. Default database passwords
2. Default applications passwords
3. External application access
4. Database direct access
5. Poor application security design
6. Incomplete patching and update procedures
7. No encryption on sensitive data
8. No change management procedures
9. No database or applications audit
10. Poor password control

## 3. Oracle E-Business Suite Three-Tier Architecture

Enterprise Resource Planning and Customer Relationship Management must be capable of collecting, processing, presenting, analyzing, and storing the data.
To collect data from the end-user, Oracle E-Business Suite includes in its technology architecture the support for two distinct user interfaces: Oracle Forms and an HTML Self-Service interface.
In addition to the user interfaces, another important function of the system is the capability to run background reporting and processing tasks through the Concurrent Processing Component.
Oracle E-Business Suite is built on a three-tier architecture: Database Tier, Application Tier and Client Tier

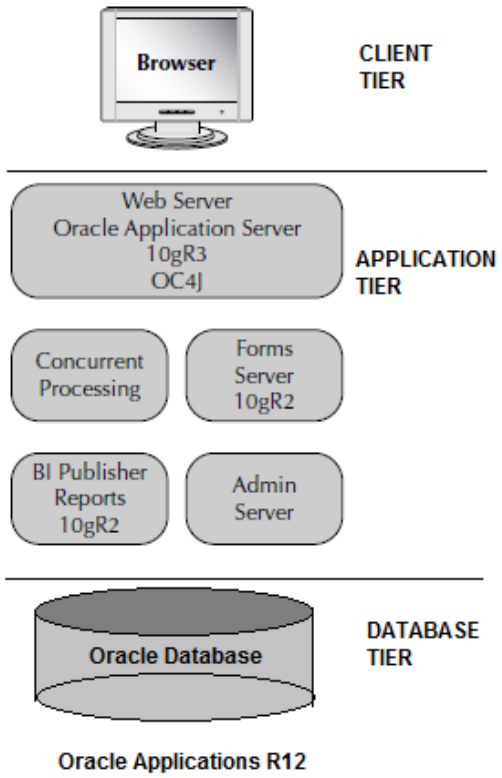


*Figure 2. Oracle E-Business Suite R12 architecture*

### 3.1 Client Tier

The client (desktop) tier is composed of two types of interfaces in Oracle E-Business Suite: Oracle Forms based or HTML-based. Both interfaces are ran from a web browser. The Forms-based applications are ran through a Java applet, Oracle Forms Client applet. The user logs in to the Oracle Applications via the web browser, through his personal home-page, the central hub to all the Oracle E-Business Suite applications.
The Oracle Forms client is similar to Windows desktop applications and is deployed as a JAR file (Java Archive) that contains all the necessary libraries for Oracle Applications Forms. After the initial download, the JAR files are cached on the browser's disk cache. The client Java libraries contain the Java classes from the Forms and Extended Windowing Toolkit (EWT), the Oracle Java library used to create and manage text boxes, tables, tabs, windows, buttons etc.

As any other Java applet, the Oracle Forms Client runs in a Java Virtual Machine (JVM). In the R11i version of Oracle E-Business Suite, Oracle used its proprietary version of JVM, called JInitiator, while in the R12 it was replaced by the native SUN J2SE Plug-in JVM.

## 3.2 Application Tier

The application tier includes the majority of application functions, including business workflow control, validation for data input on client side and many other functions. The application tier acts as an intermediary between the client tier and the database tier. As illustrated in *Fig 2 Oracle E-Business Suite R12 architecture,* the main components of the application tier are the following:

- Web Server
- Oracle Forms Server
- Concurrent Processing Server
- Reports Server (R11i version)
- BI Publisher
- Admin Server (R11i version)

In the this context, the term *server* is used to describe a logical server, not a physical machine. Logical servers can be distributed on several physical machines for performance, scalability, fault tolerance etc. and represent logical components (services) with various functions, installed on applications servers like Oracle Internet Application Server, Oracle Weblogic, IBM Websphere etc.

The web server in Oracle E-Business Suite consists of two important components: the Web Listener and the Servlet Engine. The Web Listener is also known as Oracle HTTP Server, powered by Apache. Its main purpose is to process and fulfill HTTP requests or to redirect them to other components of the Applications Server or the Oracle Applications Technology Stack.
Oracle HTTP Server is an entry point for both Oracle Forms and web-forms interfaces. For the web forms based applications, the execution of application logic and Java code occurs within a servlet engine: Apache JServ pentru R11i and Oracle Components for Java (OC4J) in R12.

The Oracle Forms Server runs the applications developed using the Oracle Forms tool. Oracle Developer 6i is used in E-Business Suite version R11i and Oracle AS 10gR2 for the R12 release.
Following the three-tier model of the architecture, the Oracle Forms Server fulfills the following tasks on each level:

- **Client Tier** – the Java Forms applet that runs on the user desktop
- **Application Tier** - Forms Listener and Forms Runtime Engine components
- **Database Tier** – data processing logic and applications data management

In Oracle Forms 6i (release R11i), the Forms listener is an executable that runs as a process (f60srvm on UNIX platforms, ifsrv60 on Windows platforms), while in Oracle Forms 10gR2 version, Forms Listener is a servlet that runs inside the OC4J servlet engine in Oracle Applications Server. The Oracle Forms Runtime process is named f60webmx (ifweb60 on Windows) and f90web in Oracle Forms 10gR2.
The main roles of the two components are as follows: Oracle Forms Listener waits for client connections, after which it spawns and manages Runtime Processes responsible with communication to the Oracle Database.

Oracle Applications allows the scheduling of background non-interactive processes, such as long-running transactions, batch-jobs, reports etc. In Oracle Applications, this scheduling is called *Concurrent Processing*, implying the idea that multiple jobs can be run at the same time on one or more nodes. This parallel approach allows resource intensive operations to be run on separate processors/nodes/servers.

The Oracle Reports server is a component of the technology stack of the R11i release. In the R12 release, the Reports Server is not present as a standalone component, its functionalities are included in the Concurrent Manager Server. The role of the Oracle Reports component is to deliver the need operational reports to the organizations.

ISSN 2067 – 4074

### 3.3 Database Tier

The Oracle Database stores applications data and database-side code, for example:

- Database Objects
  - Tables
  - Sequences
  - Indexes
- Code
  - PL/SQL code
  - Triggers
  - Views
  - Synonyms
  - Database Java code

In Oracle E-Business Suite Database design there are two main types of schemas:

Product schemas contain only data-related objects such as product database tables and sequences. For example, the module "Account Receivables" – all the data-related tables are under the ownership of the AR schema in the database.
For easier managing of the data, avoiding duplicates but at the same time sharing the content between the application modules, the APPS schema contains objects for all the modules, such as PL/SQL code, triggers, views etc. and synonyms for all the tables and sequences in the individual product schemas.
Each modules confers full rights to the APPS schema, so an user with access to the APPS schema will have unrestricted access to all the products schemas.
There are two additional schemas in an Oracle Applications Database:

- **APPLSYS –** this schema contains objects from the Oracle Applications technology stack, such as AD (administration utilities) and FND (Applications foundation).
- **APPLSYSPUB –** this schema is a special schema, used only for the initial log-in of the user for checking its credentials.

## 4. User security overview

When an user logs in, its credentials are authenticated against a table that holds the login and password details. Depending on the IT architecture, the authentication of a user can be implemented in Oracle Application or its credentials can be supplied by an LDAP provider. After the log-in, the users are presented with a list of responsibilities that in turn are assigned a menu and request group.
The security at user level is achieved through roles and responsibilities while enabling users to perform some basic, predefined registration tasks on their own.

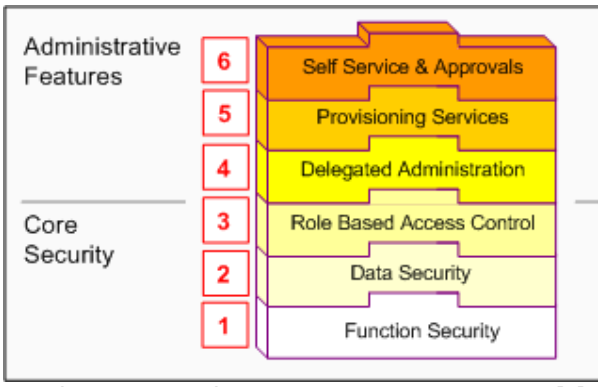


*Figure 3. Oracle User Management Layers [7]*

### 4.1 Function Security

Functional Security represents first layer of access control in Oracle Applications. Through functional security, the user access can be restricted to individual menus and/or menu options, without restricting access to data accessible from those menus.

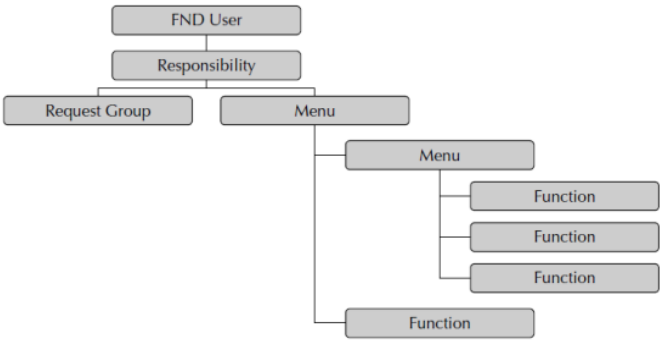


*Figure 4. Function security*

A responsibility represents a collection of business tasks, as data entry forms or reports, which the user can run or view. The responsibilities determine the user's possible actions in E-Business Suite. Responsibilities have assigned menus, which, as described in *Figure 4,* may include other menus or functions, and request groups which determine the operational reports that the user can run.
Any UI screen in the application can be associated to a corresponding function, which can be associated to a menu which the users can access through an assigned responsibility.
A request group represents a group of reports and concurrent programs that can be assigned to a responsibility. Before a user can run a report, he must have the request group which contains the said report attached to his responsibility.

## 4.2 Data Security

Going up the layers as described in *Fig 3 – User Management Layers*, the next layer is Data Security. Derived from Functional Security, Data Security provides access control to the data that an user can access or manipulate in Oracle E-Business Suite. Oracle E-Business Suite may restrict access rights to data presented in a menu, such as read-only privileges, must complete data etc.

## 4.3 Role Based Access Control (RBAC)

Data Security and Function Security help in defining the next layer, Role Based Access Control.
Using RBAC, the user security in Oracle E-Business Suite is determined by the role and responsibilities given to each user.
The Oracle E-Business Suite implementation of RBAC closely follows the ANSI INCITS 359-2004, as published by the National Institute of Standards & Technology (NIST), which defines a role as "A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role. ".
A role may be configured to consolidate responsibilities, permissions, functional security and data security policies that users need in order to accomplish a task.
Roles can be inherited, which greatly simplifies the mass update process of user rights.
As part of the RBAC model in Oracle E-Business Suite, the User Management allows the creation of Role Categories, which can be created by the application administrators in order to simplify the process of searching roles and responsibilities.
Roles can be defined in hierarchies, which can contain multiple subordinate or superior roles. Using roles hierarchies, a superior role inherits all the properties of its subordinate roles, to multiple levels of subordination.

## 4.4 Delegated Administration

Delegated Administration allows the system administrators to provide administrative privileges to users in order to simplify or separate the administrative process. With delegated administration, an organization can decentralize the administration of its users based on security subsets or organizational requirements. For example, enterprises can have users administrator for departments, regional unit etc. Delegation Policies are defined as data security policies and the delegation of administration is known as Administration Privileges.
A delegated administrator can perform actions such as: Create Role, Manage Role, Manage Role Hierarchy, Run Security Wizard, Assign Role, and Revoke Role. In older releases, administrators either had all the administrative responsibilities possible or none. Now administration operations have been granulated and administrator can be assigned a subset of privileges, which can be applied on a specific subsets of users and roles.

## 4.5 Provisioning Services

ISSN 2067 – 4074

Provisioning services represent *registration processes* that enable users the ability to have basic security actions available, such as requesting an account, a new password or additional access to the system.
Provisioning services help the application administrator to create and manage new roles and users.
Oracle User Management supports three types of registration processes: Self-service Account Requests, Requests for Additional Access, and Account Creation by Administrators.

### 4.6 Self-Service and Approvals

If required, users can perform self-service administrative tasks as registering a new account, having additional access in the system etc.
Depending on the company's business needs, custom approval workflows can be created for the self-service requests using Oracle Approvals Management engine. For example, multiple approvals from different business roles can be required before an user can enable an important role in the application.
Oracle User Management also provides basic self-service features for resetting forgotten passwords, and has the following sample self-service registration processes, which can be used in their default form or customized by the organizations in order to develop their own workflows:

- Employee Self-Service Registration
- Customer Self-Service Registration (external individuals)

## 5. Security recommendations and system hardening

Oracle clients communicate with the database using the Transparent Network Substrate (TNS) protocol. When the Listener receives a connection request (tcp port 1521, by default), it starts up a new database process and establishes a connection between the client and the database.
Recommendations:

- add IP restrictions or enable valid node checking - Valid Node Checking allows or denies access from specified IP addresses to Oracle services;
- specify connection timeout;
- enable encryption of network traffic - encryption code is already implemented in the client code, so we the server must be configured to require encryption and all the clients will follow;
- enable TNS listener password (only if required) – instead of using OS-based Authentication, a password should be set if remote admin access to the listener configuration is required;
- enable administrative restrictions;
- enable logging.

### 5.1 Oracle Database Security

This section contains security recommendations for the Database.

- disable XDB – Oracle XML Database (XDB) is not used in Oracle E-Business Suite implementations and should be deactivated, as it requires two additional TCP ports: 2100 for ftp access and 8080 for http access.
- review database links - review database links and drop unrequired or unused ones.
- middle-tier applications logon to the database through their own schemas rather than end-user accounts. System administrators should set-up their own schema for administrative tasks
- remove operating system trusted remote logon - this setting prevents the database from using an insecure logon protocol.
- implement two profiles for password management – The application administrator should use the password policy parameters to enforce password security but this could lock out applications profile from accessing the database. Application Administrator should create different profiles for application schemas and for human users.
- change default installation passwords - Oracle E-Business Suite database is delivered with up to 300 database accounts, which all have default passwords (for example, the password

for the GL (General Ledger) account is GL), all are active after installation and they can have significant privileges. Default schemas come from different sources:
    a. Default database administration schemas
    b. Schemas belonging to optional database features
    c. Schemas common to all E-Business Suite products
    d. Schemas associated with specific E-Business Suite products.
- restrict access to SQL trace files;
- limit file system access within PL/SQL - The parameter UTL_FILE_DIR limits file system access for all database accounts using the PL/SQL API UTL_FILE. Oracle E-Business Suite maintains some disk files and needs this parameter set;
- revoke unnecessary grants given to APPLSYSPUB schema;
- configure the database for audit;
- configure advanced database options such as Advanced Security.

Advanced Security is Oracle's complete security for databases which allows the encryption of data and protects both the data in the operational database and the data from backups or as it transits the network. Oracle Advanced Security doesn't need any additional configuration at the application level and provides a transparent encryption of all sensible system data, with significant benefits such as:

- integrated management of encryption keys;
- transparent encryption of sensitive columns;
- transparent encryption of the entire table space;
- HSM (hardware security module) integration.

Transparent Data Encryption (TDE) creates a new encryption key every time a column is encrypted. If more columns of the same tables are encrypted, the same encryption key will be used. Each encryption key is stored in its internal Oracle Dictionary and is encrypted itself using the master TDE encryption key. This encryption key resides outside the database in a PKCS#12 file - Oracle Wallet. Starting with Oracle Database version 11g, system administrator can save this key in an HSM device, using a PKCS#11 interface. With version 11g it's possible to transparently encrypt a whole tablespace.

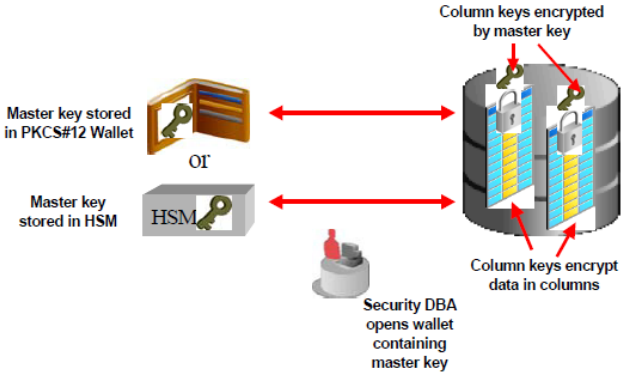


*Figure 5. Oracle Advanced Security key management.*

For an improved security, RMAN backups and Datapump exports can be encrypted. Oracle Advanced Security protects the confidentiality of network transiting data, denying man-in-the-middle attacks, data interception or data modifications. Oracle Advanced Security provides strong authentication solutions such Kerberos, Entrust/PKI, RADIUS, DCE, SSL, etc.

Oracle Application Tier Security provides:

- harden operating environment;
- harden apache configuration:
    - Remove Application Server Banner
    - Remove Unnecessary Directives
    - Remove Unnecessary Modules
    - Prevent Search Engine Indexing
- protect administrative web pages - limit web page access to trusted hosts;
- configure logging - Oracle Application Server respects Apache's logging parameters;

### 5.4 Oracle E-Business Suite Security

- strike passwords from adpatch logs;

ISSN 2067 – 4074

- set workflow notification mailer send_access_key to n - when SEND_ACCESS_KEY is set to Y, the workflow notification email bypasses the E-Business Suite sign-on process; email notifications contain an access key. The key allows the user to access the Notification Details web page directly without authenticating;
- restrict file types that may be uploaded;
- enable antispam HTML filter for uploads;
- use SSL (https) between browser and Web server;
- avoid weak ciphers and protocols for SSL (HTTPS);
- change passwords for seeded application user accounts;
- switch to hashed passwords;
- create shared responsibilities instead of shared accounts;
- configure Concurrent Manager for safe authentication - Concurrent Manager passes the APPS schema password to concurrent programs on the command line;
- configure Concurrent Manager for start and stop without the apps password;
- review and limit responsibilities and permissions;
- restrict responsibilities by web server trust level;
- set sign-on audit level;
- depending on the installation and requests, configure Audit Trail.

On the desktop level, usual security practices apply for securing enterprise desktops, which include:

- Operating system updates;
- software updates;
- up-to-date antivirus programs;
- personal firewalls;
- user security policies (password, lock-out etc.);
- disabling history and fields autocomplete.

Securing desktop terminals is a lengthy subject and not in the scope of this paper.

The enterprise Operating System Security in which Oracle Applications run is a very important part in the system's security blueprint and should be configured accordingly.

Some of the security recommendations are the following:

- cleanup file ownership and access;
- cleanup file permissions;
- filter IP packets;
- eliminate TELNET, RSH and FTP deamons;
- configure accounts securely;
- limit root access;
- secure NFS;
- disable graphical interface; there is no requirement to install X on any of the EBS servers if a remote X Display can be provided during installation;
- although not required by the E-Business Suite, the following services may provide operational convenience:
  a. NTP (Network Time Protocol) – synchronizing with a network or an external timeserver, for providing accurate audit logs simplify trouble-shooting.
  b. CRON – for operating system cleanup and log file rotation
  c. Monitoring agents – for monitoring operating system, database and application components for health and security

## 6. Conclusion

Enterprise Resource Planning Systems represent a critical component in any organization, containing data of interest for both external and internal threats and having a deep business impact in case of failure. Therefore, all security aspects – confidentiality, integrity and availability – are absolutely crucial in any ERP implementation. As with all software projects, a balance has to be made between security and functional needs of the organizations.

The multiple customizations and personalizations of ERP implementations, as required by clients in today's environment enlarge the security footprint of the system and greatly increase the number of risks and threats.

Given the complex nature of ERP systems and their importance throughout the organizations, all implementations must be carried on with respect to the industry

standards and procedures, while trying to control the amount of customization that goes in the implementation of the system.

## References

[1] Anil Passi, Vladimir Ajvaz, *Oracle E-Business Suite Development and Extensibility Handbook New*, Mc-Graw Hill, 2010

[2] Luvai Motiwalla, Jeffrey Thompson *Enterprise Systems for Management* , Prentice Hall 2008

[3] Erik Graversen, Eric Bing, *Secure Configuration Guide for Oracle E-Business Suite Release 12,* Oracle Corporation, 2012

[4] Andy Penver – Oracle E-Business Suite R12 Core Development and Extension Cookbook, Packt Publishing, 2012

[5] American National Standard for Information Technology, *Role Based Access Control,* American National Standards Institute, Inc., 2004

[6] Deloitte Touche Tohmatsu Research Team and Isaca, *Security, Audit and Control Features Oracle E-Business Suite,* ISACA, 2010

[7] Oracle, DOCs on E-Business Suite, available at: http://docs.oracle.com/cd/E18727_01/doc.121/e12843/T156458T185608.htm

[8] Oracle, ERP Seminars, available at: http://www.erpseminars.com/files/Note189367_1.pdf