Proposed Security Framework for ERP Systems

Sharafat Bibi[1], Noman Saleem[2]

[1]IT department, First Women Bank Ltd
Karachi
Sharafat.gharsheen@fwbl.com.pk

[2]SUPARCO, Pakistan
Karachi

Abstract: *The Enterprise Resource Planning (ERP onwards) systems are the dominant business software for organizations all over the world having one common database and sharing information across all part of the enterprise. But organizations using these systems are vulnerable to security threats and other complexities that range from the data ownership, change management, roles and access privileges management to the execution rights management issues. The ERP world requires a new way of thinking about security because ERP vendors are committed to provide new functionality and value to their customer. Unfortunately security is not the preventive thought. This research primarily focuses on exploring the security challenges faced by the ERP systems that fall in the category of vendor specific or indigenously developed and proposes a framework that remedies the security challenges identified.*

Keywords: *Enterprise Resource Planning (ERP), security, Oracle EBS*

1. INTRODUCTION

ERP systems are assuming increasing importance as integrated parts of business networks. They support 'E-business implementation', 'integrated activities' and 'modular architecture' for better enterprise performance, higher enterprise efficiency, and future extensions.

1.1 The Motivation Factors

First of all, the ERP systems have a focus on integration of the underlying sub-systems that does not leave these sub-systems in isolated environment. Secondly, the ERP systems are moving towards the development of network/web based applications.

Thirdly, the authorization mechanisms become more complex when all the applications get integrated. Apart from the three aforesaid issues, there are certain other issues e.g., auditing in ERP Systems, management of roles and generic security issues of ERP system.

Therefore, the security needs to be reshaped in order to get compliance with issues found in ERP systems.

1.2 Organized of Research

The objective of this research is to introduce ERP systems and explore their current state and future potentials with respect to security. The literature review provides an understanding of security of ERP systems and the weaknesses in security architectures of ERP systems like SAP R/3 and Oracle E-Business Suite (Oracle EBS). Based on investigations, we present a framework for the security of the ERP systems that provides broad vision for the ERP system developers, implementers and ERP product manufacturers.

1.3 Defining the ERP System

Information system having several software modules that share a central database, designed to automate business processes across ERP system can be defined as an 'integrated an organization.'

The objective of an ERP system is to automate the business processes of the enterprise, for the benefits resulting from this automation; that is, supporting 'e-business implementation' leading to better enterprise performance [1].

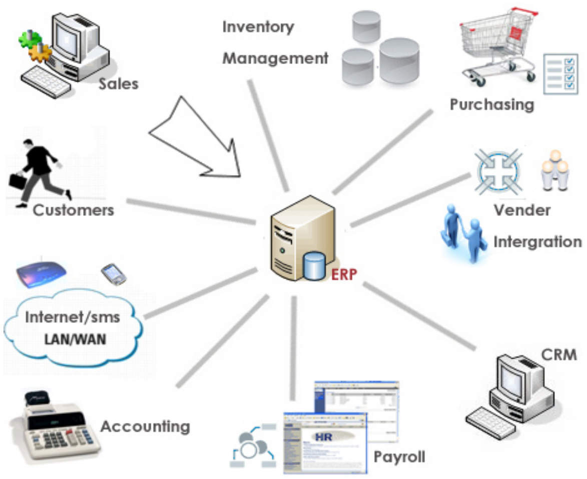

Figure 1: Typical Modules in an ERP System

The functions of an ERP system, which are associated with the 'supply chain' of the enterprise, including both its primary business activities and its support activities, are 'integrated across the enterprise' leading to higher efficiency.

2. CHALLENGES IN ERP SYSTEM

ERP systems focus on the integration of the underlying sub-systems utilizing a central data repository (an RDBMS normally). ERP systems allow its users to work on a LAN or web based environments. Moreover, the user access privileges are not limited to any sub-system rather access privileges are defined as per the duties assigned to employees; thus the ERP systems are exposed to a number of security and other challenges such as 'lack of change management', 'data ownership', 'securing custom built modules', 'complexities in managing roles', 'un-authorized information access' and 'hacking'.

The challenges in ERP systems can be categorized into two groups, namely the 'generic challenges' and 'product specific challenges'. Product specific challenges/problems are discussed in detail by focusing on two leading industry products: SAP R/3 and Oracle E-Business Suite. The generic challenges are found in all ERP products.

2.1 Internal Threats vs. External Threats

The security threats from inside the enterprise are potentially more dangerous and they have higher probability of occurrence [6]. There is a need to have proper controls implemented within the organization. We strongly recommend the view that organizations must follow the security frameworks within the organization; COBIT is one of the examples.

2.2 Application Development Architectures

Platforms provide us numerous ways to develop and deploy enterprise applications; new service oriented architectures use web services to develop self-contained, modular applications that can be interfaced very easily to create dynamic, sometimes temporary, applications. These composite applications are platform and language independent, but they expose organizations to security threats and more importantly they may not be compatible with security plans [9].

2.3 Problems due to Third Party Tools

ERP vendors often offer an 'integrated solution' that is composed of the vendor's ERP modules and a set of third party products that altogether make a complete logical system; unfortunately, sometimes the resultant 'integration' does not work well, particularly when it comes to maintaining security [4].

2.4 Lack of Change Management

Lack of change management is a major problem found in ERP products, which potentially influences security. The way modifications are done to the programs and the configurations need to be properly logged in order enables administrators to resolve security related issues. Effective segregation between development and production environments, the processes of testing, quality assurance and migration should be reviewed by the auditor.

2.5 Challenges due to Extensive Interfacing

ERP systems need to send/receive data from other systems through an integration middleware; an interface has the potential to become a weak point that can compromise security. Audit scrutiny of interfaces is one of the important aspects of ERP security reviews [7].

2.6 Challenge to the Privacy

ERP systems are such a large repository of different kinds of data that they can impact privacy issues in a significant way. Most ERP systems have a human resources and personnel module, and such modules handle a lot of data about the employees of the company. The ERP can also hold information about customers, suppliers and partners [10].

2.7 Problems beyond Control of ERP Software

If an ERP is using the integrated authentication scheme, protection of users' passwords and other credentials is the responsibility of the OS or the directory services running. Threats caused by the poor network infrastructure, switching and routing schemes, improper configuration of the firewalls or other security devices/software; viruses, spyware or other programs with similar infections may also cause serious damages to the ERP systems.

2.8 Security Requirements of Organizations

Security requirements differ from one organization to another, therefore, it would not be wise enough to draw common understanding of security for all organizations; we can plot the usability vs. security of the system:.

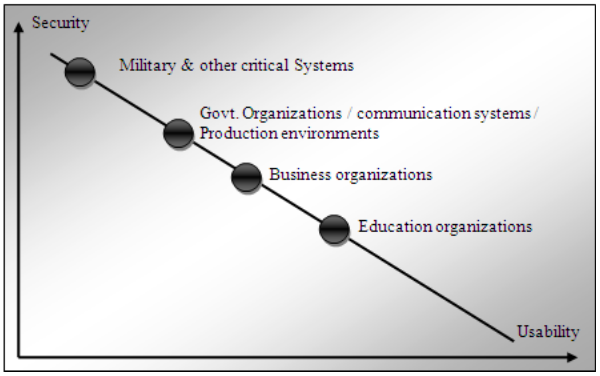
Security
Military & other critical Systems
Govt. Organizations / communication systems / Production environments
Business organizations
Education organizations
Usability

Figure 2: Security vs. Usability of the system

The more stringent security is made, the less usability is available to the end users. In ERP systems we focus on providing adequate security to the system but making it usable for the end users at the same time.

Modern systems integrate diverse technologies to implement data security. Some researchers consider that an important aspect of the security scheme is the usage of encryption to protect sensitive information while it remains stored in the database [2].

2.9 ERP Security Statistics

The Info-Tech Research Group [3] collected data from 92 different organizations having ERP systems deployed; the companies were categorized into two groups small (with 25 or smaller number of IT employees) and large (with 26 or higher number of IT employees). We have summarized their findings in Table 1.

TABLE 1 – ERP SECURITY STATISTICS

FACTOR	ORGANIZATIONS	
	LARGE	SMALL
SOME SECURITY FRAMEWORK LIKE COBIT ETC. IS BEING FOLLOWED	93%	57%
THE SECURITY FRAMEWORK EFFECTIVELY UTILIZED	27%	6%
INTERNAL AUDIT OF INFORMATION SYSTEMS NEVER CONDUCTED	11%	30%
EXTERNAL AUDIT SETUP EXIST IN THE ORGANIZATION	49%	71%
MODERATE SECURITY AUDIT SETUP EXIST IN THE ORGANIZATION	65%	28%
SECURITY EXPENDITURE HAS INCREASING TREND	56%	38%

2.10 Weaknesses of SAP R/3

The SAP authorization/security model is hard coded and we cannot further strengthen the security without having access to the source code and modifying it, and of course modifying such huge code requires a lot of effort.

One of the most important flaws in SAP R/3 is that the 'change management component' is missing which makes it impossible to trace the changes made regarding security. This becomes a hurdle if we want to audit the security of a system running SAP ERP products.

Another flaw in SAP is that it does not give us the concept of information ownership; this sometimes leads to problems and complexities regarding security. However, it is necessary to mention here that SAP uses the security objects to keep track of security.

SAP does not provide built-in security to the custom developed objects rather the developers have to write the security related code into their custom objects by themselves. This leads to the problems and additional efforts for implementation of security.

SAP supports roles; however, the security administrator is not forced to make use of purely role based approach to implement security.

The predefined or standard roles in SAP are very generic and most of the times are of no use; the reason behind this fact is that they are not made keeping in mind the requirements of any particular organization. If we use the built-in roles, it may affect the security of the system in a negative way so we should create the roles in SAP that can be easily mapped to the requirements of the organization.

Restricting users from accessing reports and program execution is not easy/simple rather it requires a lot of efforts to prevent users from accessing reports and programs they are not supposed to access.

Reassigning roles from one user to another is not easily possible in SAP, it is needed when one person is not present in the organization and his/her duties are temporarily to be assigned to someone else, so it leads to operational problems in the organization.

The security of the SAP is fully centralized, and this is once again a point of consideration whether every security related setting being centralized at one location is a good practice or SAP should de-centralize some of the security related settings. There is a weak support to determine and control duties of people, and this is due to the absence of the concept of information ownership. If we compare it with Oracle, we find that Oracle security implementation is quite simple and easy to understand for its users to plan, design and implement security [5].

2.11 Weaknesses of Oracle E-Business Suite

Oracle E-Business Suite is based on the Oracle RDBMS. However, there are some weaknesses in Oracle E-Business Suite, discussed as follows.

Oracle E-Business Suite provides a set of built-in functions that can be assigned to users as per their job description and the functionality can also be made limited for users by defining exclusion lists. However, if some functionality does not exist in pre-defined modules of Oracle E-Business Suite the developers cannot modify the code of pre-defined modules as they do not have access to the source code; hence they have to develop the custom functionality using the tools provided by the Oracle. The developers can integrate the new modules so that they are available to the end users. There is a risk of having some custom modules developed in such a way that it allows users to access data for which they are not authorized. We strongly support the view that the custom built functionality is reviewed thoroughly to check any kind of flaws before it is exposed to the end users.

Like SAP R/3, the Oracle E-Business Suite also lacks the change management component due to which it is not possible to track the changes made to security objects.

Oracle E-Business Suite lacks the data ownership in its security architecture, which leads to several post implementation problems.

Oracle E-Business Suite provides standard roles, but they are too generic and they do not fit to any organization needs.

Sometimes it may be needed in the organization to assign the responsibilities of one individual to another in case of one's absence; however, the Oracle E-Business Suite does not permit it to be done with an ease as the changes are required in user's master record.

3. PROPOSED FRAMEWORK

This section presents the framework that removes anomalies found in the currently available ERP systems.

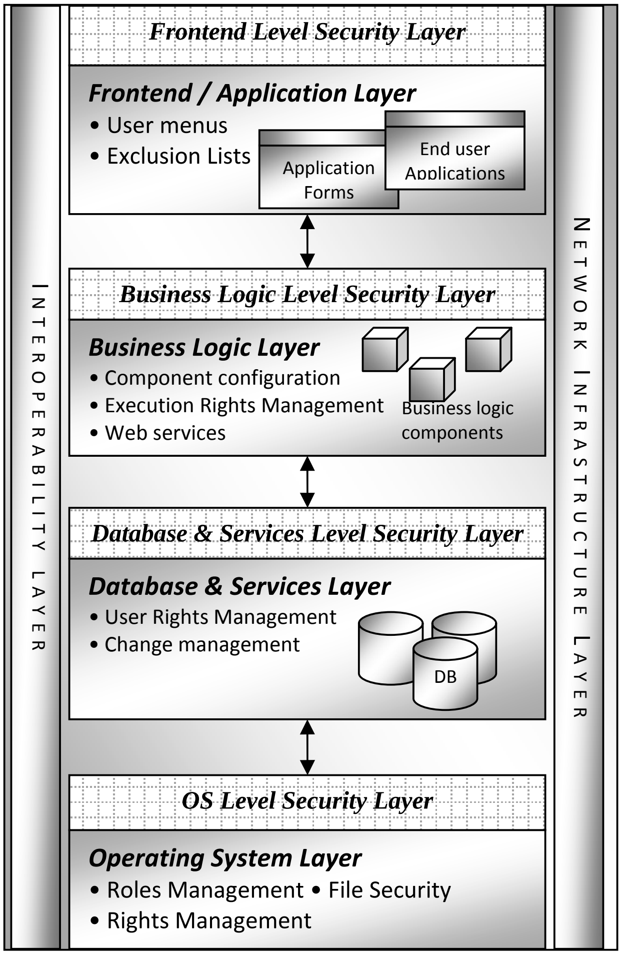
Frontend Level Security Layer
Frontend / Application Layer
• User menus
• Exclusion Lists
Application Forms
End user Applications
Business Logic Level Security Layer
Business Logic Layer
• Component configuration
• Execution Rights Management
• Web services
Business logic components
Database & Services Level Security Layer
Database & Services Layer
• User Rights Management
• Change management
DB
OS Level Security Layer
Operating System Layer
• Roles Management • File Security
• Rights Management
INTEROPERABILITY LAYER
NETWORK INFRASTRUCTURE LAYER

Figure 3: The proposed framework

3.1 Frontend/Application Layer

This layer specifically handles the tasks like:

i. Provision of frontend for diversified clients e.g., web, mobile or desktop clients.
ii. Provision of menus to users based on their privileges.
iii. Menu exclusion lists.

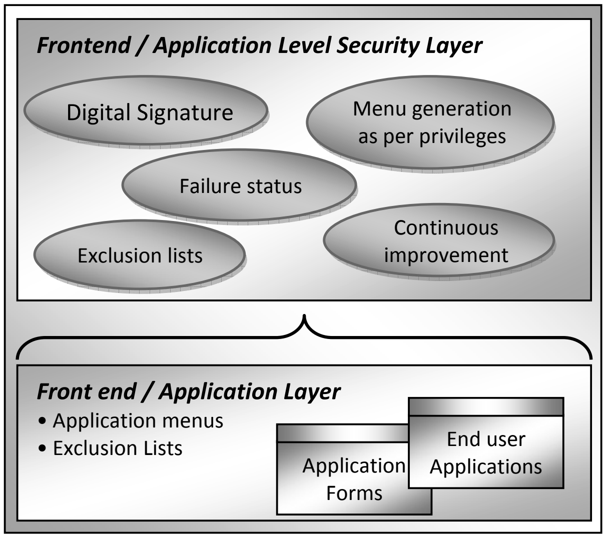

Figure 4: Front end / Application Level Security Layer

This diagram gives the structure of the Frontend/Application Layer; there exists a 'Frontend/Application Level Security Layer' which stores the entire security settings specific to the frontend and application, for example:

3.1.1 Menu Generation as per Privileges

The frontend presented to user must generate the menu as defined in the user's master record.

Recommendations: All ERP systems should have easy-to-configure facility to define menus for ERP users. More importantly, such list should be secured from unauthorized changes and any changes must be traceable. Currently the ERP systems do not support tracing changes in such objects.

3.1.2 Menu Exclusion List

This list contains the list of options to be excluded from a particular user menu.

Recommendations: All ERP systems should support menu exclusion lists, and these lists should be secured from unauthorized changes and any changes must be traceable. Currently the ERP systems do not support tracing changes in such objects.

3.1.3 Digital Signature Usage

Digital signatures are used to prove identity while transmitting sensitive information within ERP system.

Recommendations: Users must be given a provision to use digital signature whenever transferring critical information.

3.1.4 Failure Status

Some of the bad programming techniques reveal source code to the end users when some error occurs.

Recommendations: This is normally done intentionally in the development environments but when the product is ready for deployment it should be thoroughly reviewed for such flaws.

3.1.5 Ensuring Continuous Improvement of the Security

Security is normally considered a one-time investment and organizations do not allocate budget for security continuously.

Recommendations: Top level management should be committed to make continuous improvements to the security of ERP system.

3.2 Business Logic Components Layer

The complex applications running in ERP involve three layer architecture namely the frontend, business logic and the backend layer; the 'Business Logic Layer' specifically handles the tasks like:

i. Registering the components for ERP system
ii. Managing the execution privileges
iii. Integration services (e.g., web services)

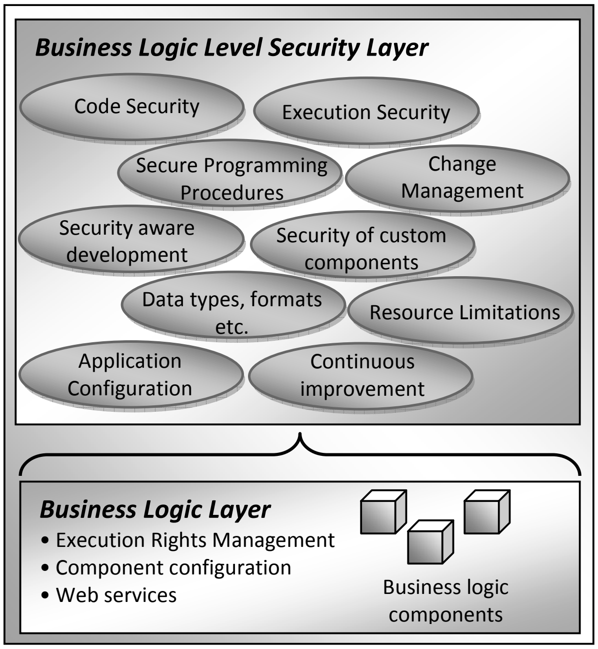
Business Logic Level Security Layer
Code Security
Execution Security
Secure Programming Procedures
Change Management
Security aware development
Security of custom components
Data types, formats etc.
Resource Limitations
Application Configuration
Continuous improvement
Business Logic Layer
• Execution Rights Management
• Component configuration
• Web services
Business logic components

Figure 5 – Business Logic Layer

There is a 'business logic level security layer' that contains entire security settings specific to the Business Logic components e.g., execution privileges. The contents of this layer typically include the following.

3.2.1 Execution Security of Built-in and Custom Components

Currently available ERP systems do not provide an easy way to secure execution of custom build objects.

Recommendations: Recommend the use of profiles to be associated with every executable object that defines its access limitations to database and other services.

3.2.2 Security Aware Development

Mostly the software developers are not the security experts; hence one cannot expect security aware software development practices to be easily adopted.

Recommendations: The security awareness should be mandatory at all levels of an ERP system.

3.2.3 Code Security of Built-in and Custom Components

There are possibilities of code injections or other similar threats in executables of ERP system.

Recommendations: Recommend the hashing technique to be adopted to ensure that there is no code injection or any other similar attack.

3.2.4 Change Management in Security Objects

The changes in the security objects are not logged which leads to serious problems in audit and traceability.

Recommendations: We recommend a change management component to be the part of security framework to keep track of all such changes.

3.2.5 Limiting the Execution of Concurrent Programs

Users can run background programs/reports while working on other applications normally which may lead to performance issues.

Recommendations: The resource usage must be restricted for users; ERP systems must have a feature to restrict CPU, memory and other resource usage. This is necessary to avoid system failure.

3.2.6 Secure Programming Procedures

Secure software development practices exist but most of the organizations do not follow such practices while developing software.

Recommendations: ERP developers must be trained for secure software development procedures.

3.2.7 Application Configuration

Every application may have its specific settings that need to be stored within the ERP system.

Recommendations: As discussed in earlier, the application modules must have a profile associated with them to store all settings of a particular module.

3.2.8 Data Types and Formats

The applications sometimes face problems if proper data types and formats are not selected.

Recommendations: Programmers should take care in selection of data types, and must be aware of buffer overflow problems and should prevent such situations to occur.

3.2.9 Security of Custom Components

Custom built components are usually not secure by default in most of the current ERP systems.

Recommendations: As discussed in earlier, all the components must have an associated profile to store all settings related to its configuration, security etc.

3.2.10 Ensuring Continuous Improvement to the Security

Security is normally considered a one-time investment and organizations do not allocate budget for security continuously.

Recommendations: A program to continuously improve security should exist in the organization.

3.3 Database and Services Layer

ERP typically accesses the database and other services being run in an enterprise. This layer specifically handles the tasks like:

i. Access to the database and other services.
ii. Integration of heterogeneous data sources.
iii. Access to the other services (e.g., authentication services).
iv. Handling users' master records.

v. Change management: It is strongly recommended that there should be a Change Control Board to evaluate the impact of each change and the changes should be properly documented and controlled.

vi. Assignment of role of one user to another in case of leave: Strongly suggests that the leave management should be integrated with the assignments of roles in ERP system.

There is a 'database and services level security layer' which stores information specific to the security of database(s) and services being accessed by the ERP system.

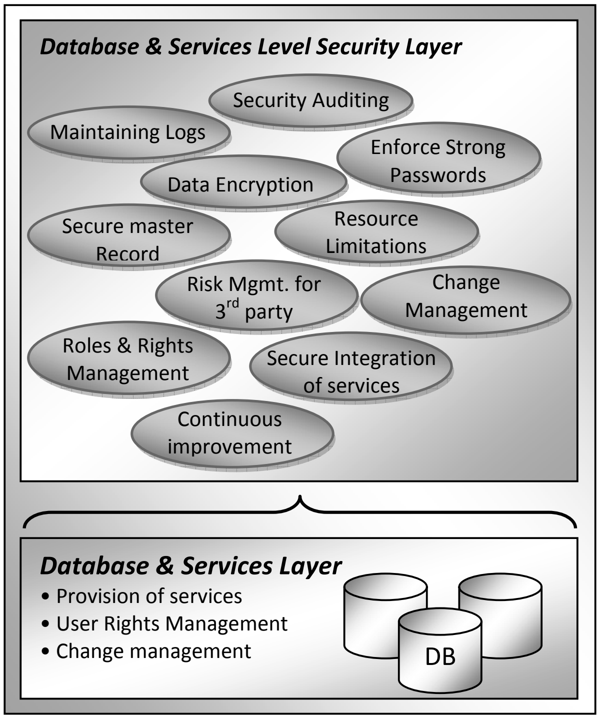

Figure 6: Database and Services Layer

The typical information stored includes following.

3.3.1 Maintaining the Logs and Tracing

Logs are very important to be maintained to enable traceability and auditing.

Recommendations: Almost all database engines support logging; however, it is recommended that the security of the logged data must be ensured.

3.3.2 Securing Users' Master Records

User master record is one of the most critical components of ERP system; RDBMS underlying the ERP system is responsible for storing this record.

Recommendations: The changes to the users' master records must be traceable and change management controls must be implemented.

3.3.3 Enforcing the Strong Password Policies

Sometimes the ERP systems allow weak passwords hence making the system vulnerable to the threat of password theft or being attacked by a brute force.

Recommendations: If the ERP is using the authentication service of database, strong password policies must be

enforced and aging and password history features must be enabled.

3.3.4 Encryption of Sensitive Data

Sensitive data needs to be encrypted while it remains stored in the database

Recommendations: Encryption must be strong enough to secure data for a minimum defined time period even if it is attached by a bruit force.

3.3.5 Ensuring the Integrity of the Data

Unauthorized persons should not make any kind of changes in the data.

Recommendations: Access control mechanism should be used to ensure access control. Row level locking mechanisms are available in RDBMS systems now a days.

3.3.6 Third Party Services

Sometimes the ERP utilized third party services.

Recommendations: If the ERP involves the third party services (software modules or others) being utilized then the following security audit considerations are to be included: Risk Assessment, Risk Treatment and Risk Mitigation.

3.3.7 Limiting Concurrent Requests made by a Single User

User may request to run parallel queries hence consuming lots of resources.

Recommendations: Hardware profiles are usually available by default in database engines like Oracle, however they are not properly configured by ERP system users, it is recommended that resource usage must be limited to an extent so that system never crashes and is able to respond all users.

3.3.8 Validation of Data

Data validation is performed at front end, business logic or back end layer

Recommendations: Data validation rules must be defined at the backend level as there are multiple applications accessing the same data and it would be quite unfeasible to validate data at front end or business logic layer, hence it is recommended that all the validation to be made at the database level.

3.3.9 Change Management

It is very necessary to have a proper change management system that controls, documents and evaluates all the changes.

Recommendations: Change Control Board should exist in the ERP system to perform all such tasks.

3.3.10 Roles and Rights Management

Database engines provide features to create roles and assign privileges to these roles based on the job description of the people.

Recommendations: Database administrators should establish roles as per the requirements.

3.3.11 Ensuring Continuous Improvement to the Security

Security is normally considered a onetime investment and organizations do not allocate budget for security continuously.

Recommendations: Continuous security enhancement is necessary to ensure the up to mark security.

3.4 Operating System Layer

This layer specifically handles the tasks like:

i. Storage services
ii. User accounts management

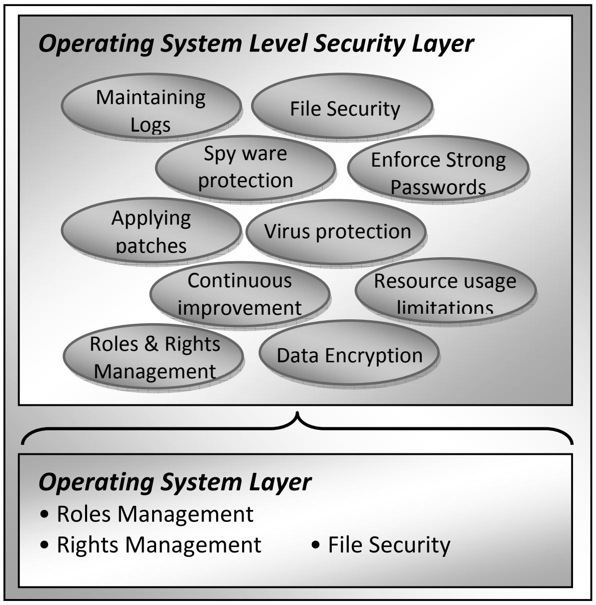

Figure 7: Operating System Layer

Our framework has an 'OS level security layer' that contains security related information specific to the operating system level; the typical information stored includes:

3.4.1 Definition of Roles, Groups and Group Policies

Every enterprise operating system allows us to define user accounts, groups and group policies apart from these OS also allow us to define Access Control Lists (ACL) to

implement security.

Recommendations: Security features of OS must be properly utilized to ensure security at end users' machines.

3.4.2 File System Level Security

All enterprise level operating systems allow administers to define access privileges to be defined on file or folder level.

Recommendations: The OS can make first contribution to the security by securing the important files at the grass root level, as everything is stored in files. Hence the file security lies at the core of the security paradigm.

3.4.3 Protection against Viruses, Worms, Trojans

Threats like viruses, worms, Trojans, code injections, buffer over flows, and execution of the data segments are common threats to the operating system that can affect the performance of any ERP system.

Recommendations: Being the lowest layer in the framework, the OS must be given the first priority while the security initiatives are to be taken in any ERP System.

3.4.4 Protection against Spyware

Spyware attack the privacy of the user (confidentiality) like key loggers, normally such attacks are launched by changing the interrupt vector tables.

Recommendations: The architecture of the operating system should be strong enough to prevent such threats.

3.4.5 Enforcing Strong Password Policies

Sometimes the OS policies allow weak passwords hence making the system vulnerable to the threat of password theft or attacked by a brute force.

Recommendations: If the ERP is using the authentication service of OS or directory server, then strong password policies must be enforced and aging and password history features must be enabled.

3.4.6 Limiting Resource Usage to Avoid System Failure

User may request to run parallel programs hence consuming many resources.

Recommendations: It is recommended that resource usage must be limited to an extent so that the system never crashes and is able to respond all users.

3.4.7 Applying Patches to Remove Vulnerabilities

OS vendors provide regular patches and service packs to prevent system from a number of threats.

Recommendations: There should be policy to update all the operating systems, it is recommended that the patches should be automatically applied to all the machines being part of the enterprise and must be controlled by a central system administration.

3.4.8 Ensuring Continuous Improvement to the Security

Security is normally considered a one-time investment and organizations do not allocate budget for security continuously.

Recommendations: Top level management should be committed to make continuous improvements to the security of ERP system.

3.5 Network Infrastructure Layer

This layer specifically handles the tasks like:

i. Provision of communication infrastructure.

ii. Allowing users to access the ERP using different modes of communication (e.g., Mobile devices, Remote sessions).

iii. Provision of security in different modes of communication.

Network Infrastructure Layer has information about the constraints on the flow of traffic over the network e.g., for critical applications it would be mandatory to use secure channel of communication while they are being accessed remotely.

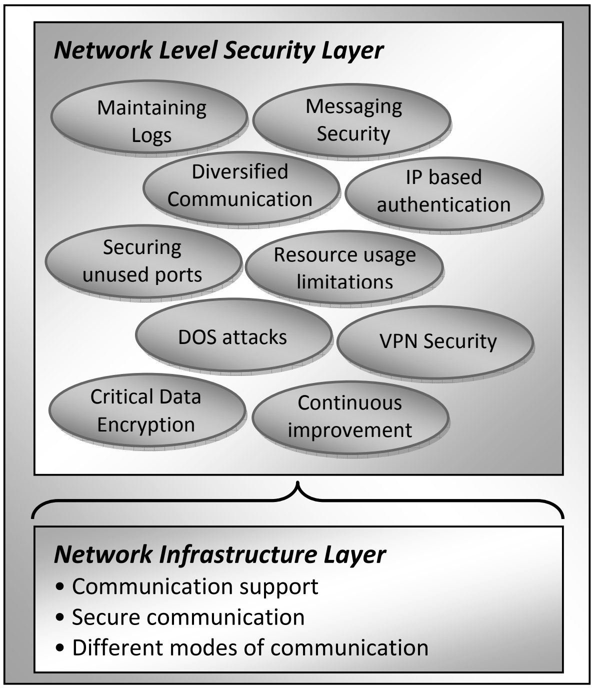

Figure 8: Network Infrastructure Layer

The security related tasks performed by this layer are discussed.

Critical Information to Flow in Encrypted Mode

In some ERP systems the password and other critical credentials flow in plaintext mode, packet sniffers can find these credentials and make potential damages to the ERP.

Recommendations: Policies must be defined to ensure that every mode of communication uses encryption to transmit passwords and other critical information.

3.5.1 VPN Support for the End Users

In today's world it is inevitable to access the ERP system remotely; users can get access to almost every resource of their ERP remotely.

Recommendations: Network administrations should ensure that users are able to establish secure channels while they are communicating remotely. ERP administrators must restrict non-secure remote access to the ERP resources.

3.5.2 Protection against DOS Attacks

The Denial of Services (DOS) attacks send too many requests to a system and as a result the system becomes unavailable to the authentic users.

Recommendations: Certain hardware and software based security solutions available to avoid such attacks; ERP systems owners should procure such devices.

3.5.3 Messaging (email) System Security

Threats like spamming can potentially decrease the performance of the ERP messaging system or workflow servers; phishing attack is also a potential threat to the users.

Recommendations: Up-to-date standards for messaging security should be adopted. Security procedures should be documented.

3.5.4 Authenticating Clients based on their IP Addresses

Some services are only accessible from the computers being the part of organizations LAN; hence computers are often authenticated using their IP addresses.

Recommendations: The computers are authenticated using their IP addresses.

3.5.5 Handling Certificate based Security

Critical servers and clients use the digital certificates to ensure secure communication.

Recommendations: Certificates should be obtained based on the organization's policy; validity of the certificates is also an important matter.

3.5.6 Limiting Resource Usage to Avoid System Failure

Some of the network Trojans and worms send enormous amount of packets to random or specified destinations and decrease the network and hence the ERP's performance.

Recommendations: Proper network security measures should be taken and applications should be allowed to access the network services based on their signature; signature of malicious programs should be added to the restricted program list.

3.5.7 Generating Logs

Logs play a vital role in tracing the activities of different users logged on to the OS.

Recommendations: Logs should be enabled as per the security requirements of the ERP.

3.5.8 Data Encryption

Data encryption features are available in modern operating systems.

Recommendations: The users of ERP should know how to encrypt the critical data, so that the confidentiality and integrity of the data is ensured.

3.5.9 Ensuring Continuous Improvement to the Security

Security is normally considered a one-time investment and organizations do not allocate budget for security continuously.
Recommendations: Top level management should be committed to make continuous improvements to the security of ERP system.

3.6 Interoperability Layer

Due to large scale integration it is very likely to happen that ERP consists of heterogeneous OS, hardware, database, applications and other platforms; this layer specifically handles the tasks like:

i. Interoperability among the services and applications belonging to different platforms/vendors.
ii. Integration services (e.g., web services).

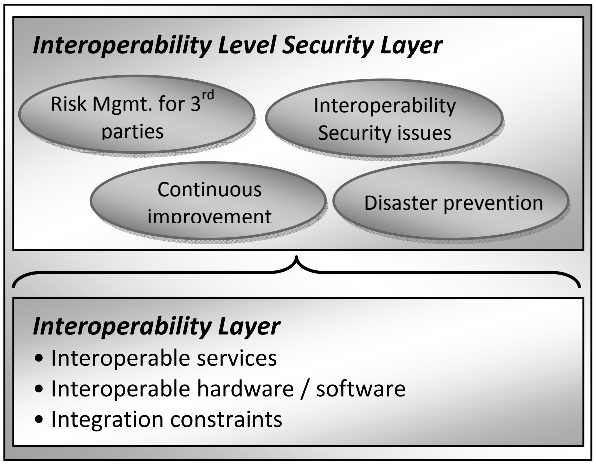
Interoperability Level Security Layer
Risk Mgmt. for 3rd parties
Interoperability Security issues
Continuous improvement
Disaster prevention
Interoperability Layer
• Interoperable services
• Interoperable hardware / software
• Integration constraints

Figure 9: Interoperability Layer

This layer also stores the security information specific to the interoperability.

3.6.1 Risk Management for Third Party Services

Since ERPs are large scale systems they utilize the services of hybrid platforms and vendors. ERP vendors also offer packaged products that contain third party products; organization may also procure third party software add-ons to be used with their ERP systems.

Recommendations: All such products / services must thoroughly go through the Change Control Board before their implementation.

3.6.2 Managing Security Issues due to Interoperability

As discussed above, the ERP systems utilize third party software / services hence it also exposes the ERP system to the new security vulnerabilities due to third party involvement.

Recommendations: It is strongly recommended that security of such software/services should be thoroughly reviewed before implementation.

3.6.3 Disaster prevention due to Interoperability

Incompatibilities and inconsistencies may lead to unavailability or even disaster of the system.

Recommendations: The services or products should be tested for the compatibility and consistency before being integrated.

3.6.4 Continuous Improvement

Procedures and processes for the interoperability need to be continuously monitored and updated within the organization.

Recommendations: Continuous security enhancement is necessary to ensure the up to mark security.

4. CONCLUSIONS

Security is an afterthought in most of ERP system implementations that leads to several problems. A lot of work in the area of security has already been done, and the stakeholders of ERP system need thorough understanding of security needs at different levels as depicted by our proposed framework. Secondly, commitment of executive management to implement and fund security initiatives matters a lot. There is a misunderstanding that the domain of security is only limited to a particular group within an enterprise. If we thoroughly consider each security sub layer we can easily draw a conclusion that security awareness is a mandatory requirement for every employee of an enterprise. We strongly recommend the continuous improvement to be achieved in each sub-layer to ensure that ERP is secure and can defend any new challenge.

This study has proposed a security framework particularly for ERP applications. This framework has developed preventive measures that would be used in future development of ERP applications. The main aim is to secure the layers of the ERP application that include database layer, business layer, and presentation layer.

5. FUTURE WORK/OPEN ISSUES

This proposed framework has covered the security issues related to ERP systems. Implementation of this proposed framework in developed ERP systems would require extensive efforts. A proposed approach is to develop sub-layers and specific practices related to the layer that will help in the implementation of the proposed framework.

REFERENCES

[1] Ali Haj Bakry, Saad Haj Bakry. ‘Enterprise resource planning: a review and a STOPE view’, International Journal of Network Management, 2005 John Wiley & Sons, Ltd.

[2] J. Saúl González-Campos. ‘Secure Groups: Enhanced Management of Encrypted Data in Databases’, Seventh Mexican International Conference on Computer Science (ENC'06), 2006, 0-7695-2666-7/06.

[3] Info-Tech Research Group. ‘Mind the ERP Security Gap’, June 28, 2007, www.infotech.com.

[4] Joy R. Hughes, "ERP Security Checklist", Vice President for Information Technology and CIO George Mason University, jhughes@gmu.edu, Copyright© 2007.

[5] Manfred Paul. ‘A Reference Framework for Security in Enterprise Resource Planning (ERP) System’, Ph.D. Thesis, Faculty of Science, University of Johannesburg, August 2005.

[6] Roberta S. Russell ‘A Framework for Analyzing ERP Security Threats’, Euro-Atlantic Symposium on Critical Information Infrastructure Assurance, March 2006.

[7] S. Anantha Sayana. ‘Auditing Security and Privacy in ERP Applications’, Information Systems Control Journal, Volume 4, 2004, Information Systems Audit and Control Association, www.isaca.org.