Role Based Access Control

Lalit Bhangale

A Patni White Paper

COPYRIGHT

Restricted Rights Legend

Information in this document is subject to change without notice and does not represent a commitment on the part of Patni. This document is provided "as is" without warranty of any kind including without limitation, any warranty of merchantability or fitness for a particular purpose. Further, Patni does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the written material in terms of correctness, accuracy, reliability, or otherwise.

Patni Computer Systems Limited

India

Akruti, MIDC Cross Road No.21
Andheri (E), Mumbai 400 093
Tel: +91 22 5693 0205
Fax: +91 22 5693 0211

North America

238 Main Street
Cambridge MA 02142
Tel: +1 617-354-7424
Fax: +1 617-876-4711

UK & Europe

Vistacentre, 50 Salisbury Road
Hounslow, Middlesex, UK. TW4 6JQ
Tel: +44 20 8538 0120
Fax: +44 20 8538 0276

Japan

4th floor, Aoyagi Building, Chuo 5-39-11, Nakano-ku, Tokyo 164-0011
Tel: +81 3 53281952
Fax: +81 3 53281951

Table of Contents

INTRODUCTION

An expansion in corporate profiles, as a result of mergers and strategic alliances, tends to dilute geographical boundaries in contemporary businesses. Organizations today have assumed a global presence and are no longer restricted within their narrow confines. Consequently, Internet with its ubiquitous presence in intra and inter-organizational communication has emerged as a vital component in modern business paradigm. Business houses, in recent years indicate an increasing affinity towards it to effectively:

- Acquire new customers
- Acquire new partners
- Use partner's infrastructure
- Combine Intranet and Extranet

The increase in user list has led to a corresponding increase in the demand for resources. These users can be Internal, External, Contractors or even Business Partners. Moreover, the access for each of these users to the resources may vary. Organizations are increasingly under pressure to accommodate their ever-expanding user list. Introducing an array of different and complex set of applications, operating systems and databases however has led to further complicating matters.

Typically, each application system has its specific user administration control and is managed by respective system administrator. Administrative effort and cost is considerably increased. This is because owing to the change in need of business, more new applications are added. As each application system can behave differently than others, there is a lack of common user privilege policy.

When a new employee joins the organization, the user may be created into HR Database, E-mail System, Payroll System, ERP System and so on. (See Figure 1)

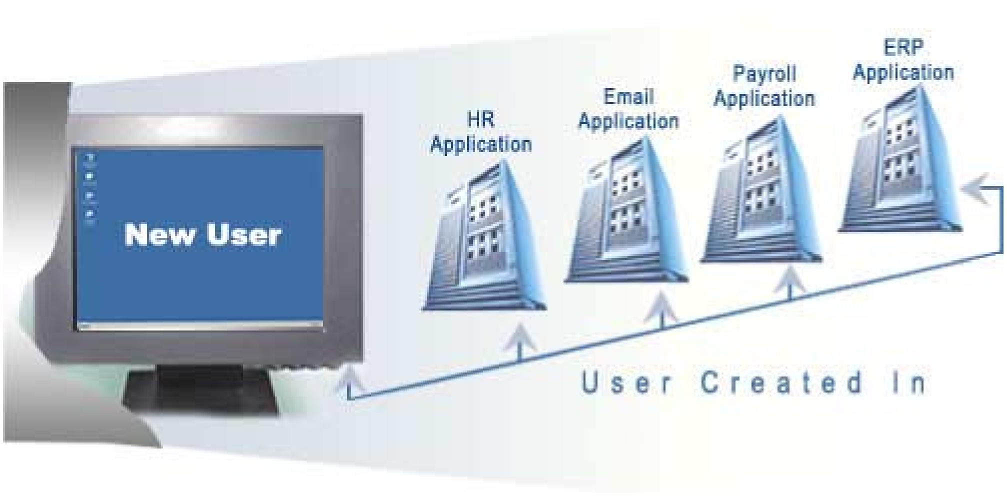

Figure 1: Employee as user

Different administrators maintain the users lists, giving rise to duplicate, and at times, inconsistent user entries. If user records in one system are updated, there is no way to communicate this to the other system.

Moreover, organizations extend the application resources to Intranet and Extranet (or Internet) users. This has led to controlling user access to information and other resources becoming even more important and complex. For such organizations, there is an immediate need to develop and enforce access policies that protect sensitive and confidential information.

This leads to the need of E-Security infrastructure within the organization. Typically, a security solution should be able to address,

- User Authentication which verifies users claim of identity
- User Access control, which determines what applications, services and resources are available to an authenticated user
- Policy based User Authorization, which allows organizations to enforce the policy for each user to see the type of contents and the privileges of the user to access the resources.

Role Based Access Control (RBAC) is method of assigning access to resources within organization, based on the individual's need for the data information.

This white paper discusses important concepts related to RBAC and its implementation.

NEED OF RBAC

The need to control access results from the Job Function or Role of the user within the organization. RBAC allows Security administrator to configure the access of user, based on policies set within the organization. RBAC decreases the cost of network administration, while improving the enforcement of network security policies. The challenges in RBAC stem out of following reasons:

- **Number of Applications & Systems**
  The applications are many and are characterized by different operating systems and platforms. Moreover, they may be changed frequently, to adapt to the dynamic nature of the business.

- **Dynamic Growth Leading Increased User Base**
  Organizations allow internal user and external users (Remote Users) and business partners or merged business organizations to access their applications. Every time an application is accessed, user Identification is very important.

- **User Administration Cost**
  The cost of administering users for all the applications is huge. The dependency on the administrative staff increases.

- **Productivity Cost**
  The manual process of user authorization takes a long time, thus reducing the productivity.

- **Need to Centralize User Control**
  User management is becoming complicated, especially with geographically separated applications and users. There is a need for centralized schemas rather than individual applications authentication and user authorization.

- **Applications are accessed 24 x 7 x 365**
  The growth in remote access is increasing security worries. The applications are used round-the-clock by teams working in many time zones. It is important to note that the access to the rightful users is not compromised for the sake of ease of administration.

- **Security Breaches with Lack of Centralized Control**

Role Based Access Control is need of today's business. Without RBAC, organizations pay more, and yet run some serious business risks. Some risks can adversely affect the organization's objectives and performance.

Lack of centralized user administration increases efforts and cost of managing user accesses. Human errors can lead to security breaches.

- **Regulatory Requirements**
  Depending on the nature of business and the country where it operates, the organizations may be required to maintain security mechanisms that comply with regulatory policies. These policies generally require the basic information to be shared, while restricting only specialized information depending on work delegation.

- **User Satisfaction**
  The load on help desk to support users (with issues like passwords) is more.

UNDERSTANDING ROLE BASED ACCESS CONTROL

ROLE BASED ACCESS CONTROL (RBAC)

In RBAC, the access privileges of each user to all the resources, applications or services are linked with "Role" of that user (see figure 2).

In RBAC, the access privileges of each user to all the resources and services are linked with "Role" of that user in the organization.

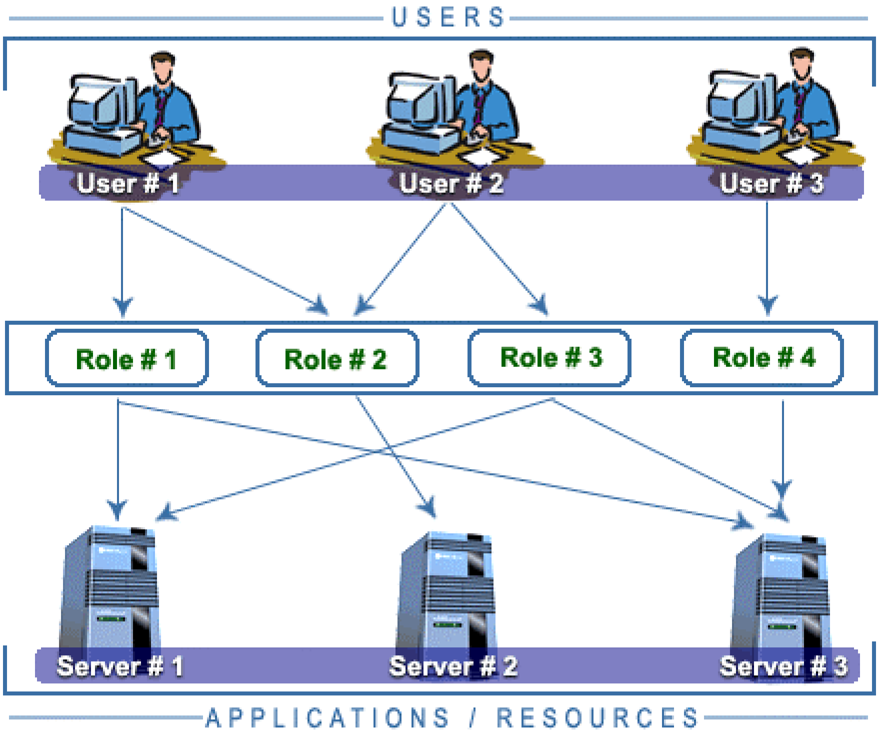

Figure 2: RBAC Principle

The role may represent the job functionality or organizational hierarchy. Each role shall then be given permissions. For example, a role called "Payroll Clerk" may have all the access privilege and permissions associated to fulfill the job function "Clerk" within "Payroll Department".

Due to the nature of varied responsibility of performing job functions, one user may be associated with one or more number of roles.

A typical organization may be having the roles defined by

- Department
- Position
- Authority
- Location or
- Special Assignments or Functions

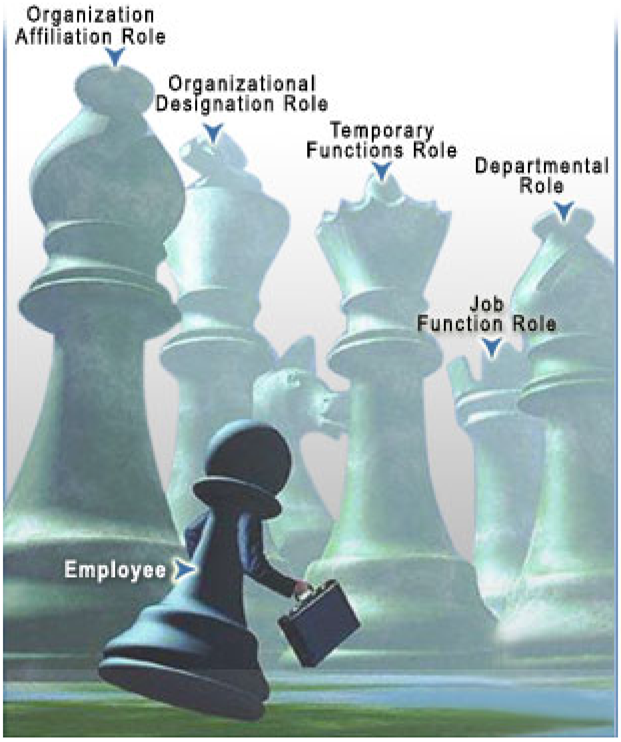

Figure 3:Various roles of a person

The privileges associated with the role may be dynamic or context based in nature. For example, “Payroll Clerk” role may have privilege for certain time period or for certain location.

BENEFITS OF RBAC

Role based access control has many significant advantages over the conventional user-based access control systems.

- RBAC simplifies the user administration procedures by centrally collating the user definitions, access permission assignment and audit trails.
- Access permissions are attached to roles. Hence the modification in such procedures have to be carried out only for Roles not for users. Thus it saves a lot of administrative work and time.
- User provisioning and de-provisioning may be done automatically, with modified workflow systems. This makes provisioning or de-provisioning of the user, a single administrative process.
- The information exposure is restricted to that needed by the role of user. Hence, excess information disclosure to users can be avoided.
- Enforcing the organizational security policy is easy, as provisioning and de-provisioning audit trails are instantly available.

- RBAC results in huge cost savings, as Administrators are required to manage only one centralized system.
- Business continuity and disaster recovery functionality can be achieved very fast with RBAC.
- RBAC may be able to provide the regulatory compliance be required for specific types of business (for example, requirements mandated for Healthcare by the HIPAA act).

HOW RBAC FUNCTIONS

A simple process flow of role based user access control, is shown in figure 4.

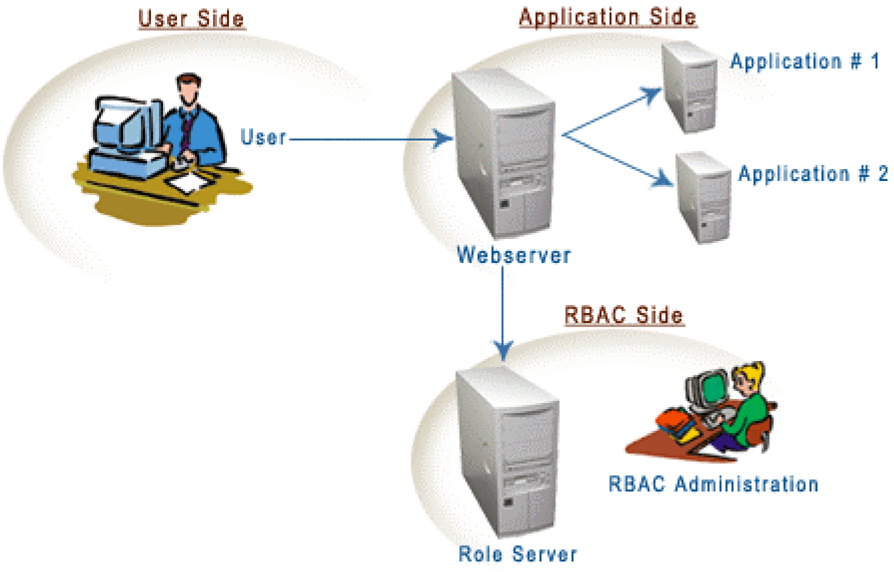

Figure 4: RBAC Operation

In RBAC, the web server fetches role information from Role Server and applies Authorization logic to provide access control the user.

The user uses web browser to connect to the application. The web server redirects the user to directory-based server, containing the user profile data and application services data. After successful authentication, based on the role attached to the user, the user can use the required application component. Web server fetches the role information from Role Server and applies the authorization logic to authenticate and authorize user’s access rights.

Components of the solution

- **Client side**
  The client uses web browser to connect to the application. A user-id and password will be issued to the Client for connecting to the application.

- **Web Server**
  The web server serves as presentation layer for the application, having web pages to be presented to the user for authentication and data formatting. The Role-Permission Matrix, used to relate the relationship between Role and its access permission, is also a component of the web server.
  For better security purposes, the web server shall also have the Secure Socket Layer (SSL) enabled connectivity. This helps to provide the session level security for each client side

connection to the web server.

- **Role Server**
  The role server shall be having the user related data for user authentication, user role assignment and user permission levels. The matrix with each user with related role information should be used to attach the roles to the user. The user may be having one or more number of roles.

The process of user connecting to the application may involve following steps.

- User tries to connect to application using browser.
- The web server presents the user a form to provide the authentication details (like user-id and password).
- User completes the form.
- The user authentication information is then securely transmitted to web server.
- The web server then redirects the user authentication credentials to Role server to authenticate the user.
- The web server may use Common Gateway Interface (CGI) scripts to invoke the connection to Role Server. The purpose of this redirection is to authenticate the user and retrieve the user role information.
- The successful authentication from Role Server results in retrieval of user-id and associated information back to web server.
- Web server validates this user role information with the Role-Permission Matrix and allows the user the application access.

LDAP Based RBAC

The Role Server can be effectively implemented using directory server products. Ideally the directory server can contain the variety of information for

- User authentication
- User authorization
- User personalization
- User access to organizational resources

The directory server can be chosen as single centralized repository which may contain user profile with Authentication, Authorization, Personalization details. Based on the business requirements and information security policy, a directory structure (schema) can be defined. Most of the directory servers have a standard structure and mostly compatible with each other. The enterprise applications having the ability to user LDAP can be easily integrated with such directory server, eliminating the need for having application specific authentication and authorization databases or repositories

Since directory servers are optimized for read operation using LDAP, it is ideally suitable for retrieving the user profiles, personalization and other details needed by the application.
With the features like referral and high scalability, LDAP based role based server implementation, can be the choice for the future.

Implementing RBAC

RBAC implementation should start with answering following questions.

- What types of Roles are to be created?
- Who will create the Roles?
- How will the Roles be created?

- How will the Roles be related to the Systems / Applications?
- How to map the users with the Roles?

The directory server with LDAP can support the organizational hierarchical structure as part of role definition.

Figure 5 shows typical roles in an organization .They are assigned to one or more users.

Identifying roles correctly is a key to implementation of RBAC.

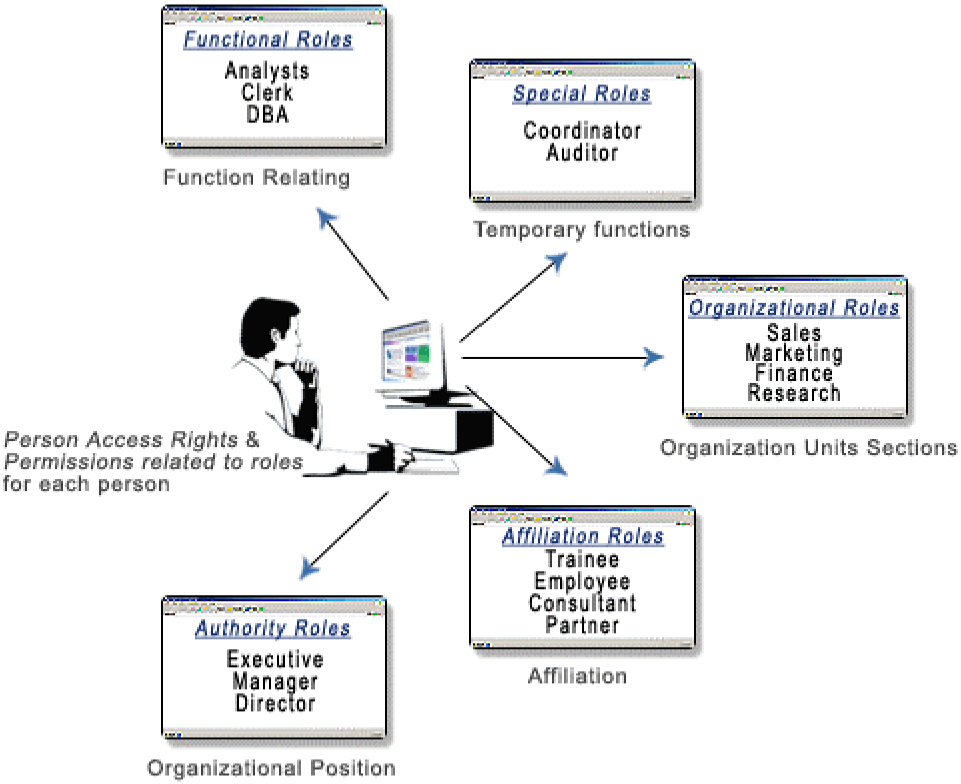

Figure 5: Typical roles Assignments for a person

CREATING ROLE SCHEMA FOR DIRECTORY SERVER

The Roles are created in the directory and then assigned to the users.

The schema for the directory server needs to contain additional branch “Roles”. It contains the roles as defined by the organizational job functionality and business processes.

To add the assigned roles and user to roles, the directory server schema is added with two extensions. One extension is to have the role ID definition and other for the role.

All the commercial directory server, do have the standard object class as
Person--> OrganizationPerson -->inetOrgPerson

It is added with object class as “RoleID” to allow the user to be assigned with the roles.

Two key steps in implementing RBAC are, creating roles schema and assigning roles to users.

Assigning Roles to User

An organizational user may be having more than one role assigned as a requirement. The user record shall be added with the “Role Attribute” field. This field is provided with multiple values, which indicate more than one role assigned to the user.

RBAC- ACCEPTABILITY AND ADOPTION

Any organization making use of a computer network for limiting access to a specific information is most likely to implement RBAC. A few of the possible areas are highlighted below:

I. Banking
II. Healthcare
III. Government
IV. Software Development
V. Defense.

In all the organizations mentioned above, Information Security is a principal part of their operations.

A survey was conducted by NIST – Program Office Strategic Planning and Economic Analysis Group around March 2002, to check the consideration / implementation for RBAC at company level. It reveals the following data.

Status	Percentage
Companies considering adopting an RBAC system	42%
Companies in the process of designing an RBAC system	8%
Companies currently implementing an RBAC system	12%
Companies having RBAC system in operation	12%
Companies having no plans to adopt an RBAC system	27%

However, the report also opines that organizations featuring organizational, staffing and Data traits are the prospective users of this technology. Moreover, it has also identified certain other traits in organizations, which make implementation of RBAC imperative. These include:

a) Limited security resources
b) Stable organizational structure
c) Maximum control over IT resources and data
d) Huge workforce with high turnover rates

LIMITATIONS OF RBAC

RBAC also reveals certain drawbacks. Some of them have been enumerated below:

1. Re-engineering Security Administration: Business Process for security administration needs to be re-visited for each application.

2. Role Engineering: Role definitions should be simple and consistent so that each application integrates easily. This is a manual effort and may incur additional cost.

3. RBAC Design: The design of RBAC system can be complex especially with the environments including heterogeneous platforms, multiple application and location separation.

4. Information Security Policies: The policies may require the additional modification to adopt RBAC to take care of Job Separation and Need to know privileges.

5. Migration Costs: Every application may not support the concept of RBAC, so it may be required to rewrite, scrap or replace.

6. Return on Investment: It is difficult to approach, as RBAC is a concept which may be associated with all the applications, platforms and business processes.

7. Lack of availability of products: Lack of available products to support RBAC which may involve roles with user attributes, location attributes and context based attributes.

PATNI SOLUTION

At Patni, we realize that an enterprise IT infrastructure is the backbone of business today. Hence our Enterprise Systems Management (ESM) practice is based on the four fundamental blocks that govern any IT infrastructure:

- IT Strategy
- IT Infrastructure Management
- IT Service Management
- IT Governance and Compliance

Patni has extensive experience in managing the IT infrastructure of several Global 2000 customers. We have built significant expertise in the areas of systems management, applications management, systems integration, business continuity and helpdesk management. Our ESM practice' service offerings are grouped into three categories.

Managing Services	Management of Data Center, Desktop & Server, Storage, Applications, Database, Network, Messaging Systems and Technical Helpdesk
Professional Services	Consulting and Implementation Services
Security Services	Designing, Implementing and Monitoring Security Infrastructures

The Information Security Services group works exclusively to address the critical security needs of organization, Policy and Procedure compliance. It also looks into the implementation of security solutions. As a consequence, Patni has developed value-added services as part of its Identity Management solutions (IMS). A few of its features are mentioned below.

- Feasibility Case Study for Organization for IMS.
- Scoping business and technical requirements for IMS.
- Policy and Procedures with Business Mapping
- Role Definitions and User – Roles Matrices
- IMS Technology Selection
- IMS Integration
- IMS Awareness and training

These services help in the efficient deployment of identity management solutions. The figure given below helps in illustrating the components of IMS:

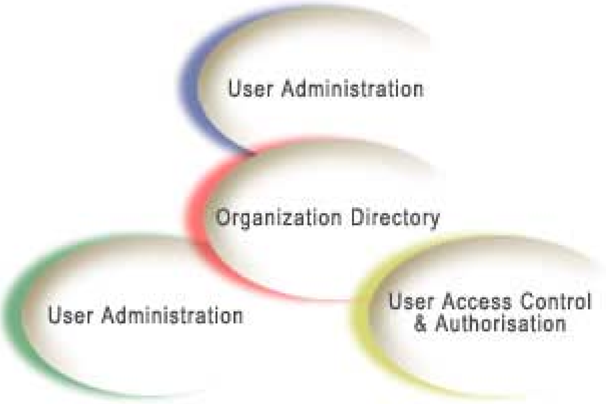

Figure 6: IMS Components

For the Implementation of IMS, Patni utilizes the PLOT methodology. It involves:

- **P**rocesses (Methodologies, Standards and Best practices)
- **L**aboratory (Patni Knowledge base)
- **O**rganisation (Trained and Certified consultants) and
- **T**echnology (Technology expertise and Partnerships)

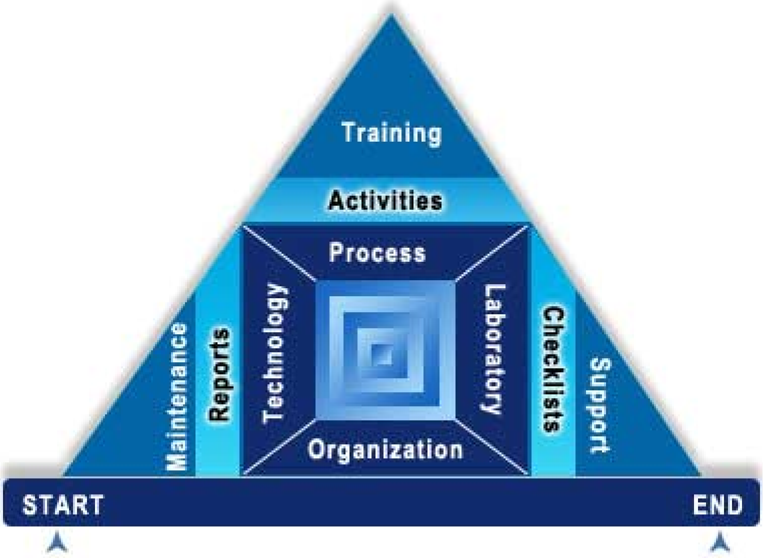

Figure 7: PLOT Methodology

The Patni PLOT methodology for system security design and implementation consists of five simple sequential steps as detailed below.

Step 1	**Requirements**	This step consists of gathering the security requirements of the project. It will also include the standard compliance requirements like COBIT, BS7799 etc. Further, it includes project planning, requirements analysis and the PLOT analysis for the project.
Step 2	**Design**	It includes the design of the security framework, customization of the standards and industry's best security practices for the project, system architecture design and a

		security test strategy for the project.
Step 3	**Integration**	It consists of customization / development and integration of the security subsystem with the application resources and other IT systems. This step is essential to ensure that the security systems inter-operate with other IT systems.
Step 4	**Deployment**	This step consists of deploying the security solutions and testing them.
Step 5	**Post Deployment**	This step consists of the audit of the security system to test whether they comply with the requirements. Further, this step will also cover an analysis of future requirements and their impact on the security systems. It also includes the change control management and support.

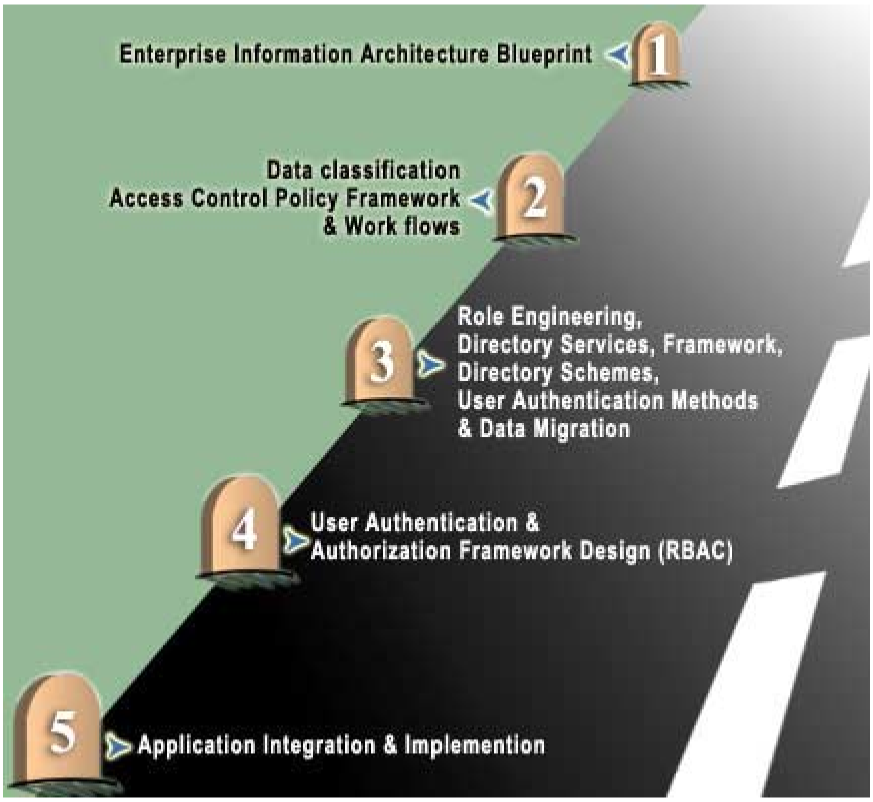
Enterprise Information Architecture Blueprint
1
Data classification
Access Control Policy Framework
& Work flows
2
3
Role Engineering,
Directory Services, Framework,
Directory Schemes,
User Authentication Methods
& Data Migration
4
User Authentication &
Authorization Framework Design (RBAC)
5
Application Integration & Implemention

Figure 8: Milestones for IMS Implementation

The methodology has the following steps.

1. Define simple milestones
2. Define tools for each milestones
3. Use predefined templates
4. Support for entire project life-time cycle

Some of the advantages offered by Patni are mentioned below:

- Patni possesses proven methodology for solution implementation and Project Management. This is an added advantage for the system since it requires the infrastructure to ensure automation in Workflow Systems.

- Patni offers a combination of IT knowledge and security expertise. This is evident in the profound business understanding, technically well equipped Network Operations center for 24 x 7operations and proven support systems mechanisms.

Business Value

Patni has implemented RBAC for one of the largest soft drinks company. The main **business drivers** were identified as

- The need for a centralized access / authorization,
- Enforcement of Information Security Policy to access data as per data classification
- Audit compliance
- Simplify the User administration.

The Patni team started work as consultants to Business and Technical requirements based on Identity Management Framework. The **scope of activity** included devising Role Based Access Control model, devising User provisioning methodology, establishing a centralized user repository as well as a user authorization repository. It also included the implementation of the solution and an Application security model with Identity Management across applications.

The **customer benefits** from this implementation included simplification of user provisioning process, reduced operational cost, compliance with Information security policy, enforcement of need to know /need to access processes delegated administration with onshore- offshore model.

CONCLUSION

Computer Based Access Control predominates contemporary technical jargon. It connotes restricting access to a specific system not only on the basis of who or what process but also the type of permission granted. Role Based Access Control is another addition to the existing technical lexicon. It refers to controlling user access on the basis of roles. Modern day businesses, having transcended cultural, linguistic and geographical barriers, display a growing inclination towards adopting the mechanisms of Role Based Access Control (RBAC) in their operations. Controlling User access, in their view is the essential step in ensconcing the benefits of E-Security measures in their system. Organizations from various spheres including Networking, Banking, Insurance, defense or even Healthcare are only too eager to embrace the benefits offered by it.

Suitably equipped with various advantages to its credit, Role Based Access Control technology is well poised to reduce the potential problems faced by businesses for application management and user access control. It helps organizations to allow users to access the application and resources on need-to-know basis and according to their job functions. Moreover, RBAC will help organizations requiring regulatory compliance to the acts like HIPAA and others.

ABOUT THE AUTHOR

Lalit Bhangale

Lalit Bhangale is a Certified Information Systems Security Professional (CISSP) and has been an Information Security technical consultant and security architect.

His information consulting experience covers areas such as Application Security and Network Security with proven expertise in Identity Management Solutions, Public Key Infrastructure Solutions, Directory Server (LDAP) Solutions, RBAC Methodologies, Information Security Strategy, Audits and Business Continuity Planning.

His product consulting experience cover solutions for Access Control and Encryption & PKI solutions from Baltimore Technologies, RSA and Gemplus, PKI Middleware Solutions from KyberPASS Corporation, Directory Solutions from Critical Path and Microsoft and Network Security Solutions from Cyberguard Corporation, Redcreek Corporation, Symantec Corporation.

ABOUT PATNI

Patni is a global IT Consultancy and Services provider with revenues in excess of US $188 million (Rs. 914 crores) and over 5600 professionals. Our six offshore development facilities and more than 20 international offices offer strategic advantage to several Global 2000 companies.

Patni delivers high quality, reliable and cost-effective software solutions to customers in the Manufacturing, Insurance, Banking and Financial Services, Retail, Hospitality, Energy and Utilities industries. Our focus areas include eBusiness, enterprise applications, embedded solutions and enterprise systems management, while our service offerings comprise of Business Process Outsourcing, re-engineering, application development and support. These capabilities are complemented by our alliances with leading software vendors -- Microsoft, SAP, Oracle, BaaN, Siebel, BroadVision, and Interwoven.

An ISO 9001:2000 certified organization; assessed enterprise wide at SEI-CMM Level 5 and PCMM Level 3, Patni has also integrated Six Sigma techniques to focus on continuous, measurable process improvements.

GLOSSARY

RBAC – Role Based Access Control

HIPAA act- Health Insurance Portability and Accountability Act of 1996

LDAP- Lightweight Directory Access Protocol

CGI – Common Gateway Interface

NIST - National Institute of Standards & Technology

PLOT Methodology- Methodology involving Processes, Laboratory, Organisation, Technology.

IMS – Identity Management Solution

ESM- Enterprise Systems Management