The Secure Role Based Mission System (SRBMS)

EDUARD BABULAK*†  
Member,  
Computer Science and Engineering Department of Informatics and Natural Sciences  
The Institute of Technology and Business,  
Czech Republic  
Corresponding author: babulak@ieee.org

WAQAS AHMED‡  
Non-member,  
Department of Computer Science  
Maharishi University of Management,  
N 4th Street, Fairfield, IA, 52557 USA  
bitguider@yahoo.com  
yartoo@163.com

CEN DAI‡  
Non-member  
panchen0207@gmail.com

AMANUEL HAILU‡  
Non-member  
amaghya@gmail.com

(Received October 5, 2015, revised December 18, 2015)

Abstract: Given the current and future development of computerization and information communications infrastructures, the organizations are facing more and more challenges how to secure their information asset and information flow within the organization and globally via Internet. The ubiquitous access to Internet introduces new challenges for secure access control systems providing access authorization at any-time, from-anywhere and by anyone.

This paper discusses the development of Role Based Access Control (RBAC) used for a secure web system. The proposed system authenticates the authorized users according to their level of trust, while providing them with proper access to a specific task(s) or assignments(s) within the organization.

The SRBMS is an extended RBAC model facilitating an alternative ways to distinguish between the user authentication and access hierarchies. It keeps track of logging, while back-tracking the recent activities performed by the authorized personnel accessing on-site or remotely the online resources via web interface.

The paper present an enhanced RBAC model which provides the user authentication and authorization based on their position and function within the organization. While being consistent with the ANSI RBAC standard, the SRBMS model provides secure access to online resources based on user’s specific roles within the organization via secure web-interface facilitating a restricting account access to authorized users only.

The main contribution of the paper is to provide solution to protect any government, military or business organization, which utilizes Web-URL Security with Database Level Security.

Keywords: Computer Security, Role Based Control Access; Secure Role Based Mission System; Web and Database Security.

1. Introduction

Given rapid development and ubiquitous access to Internet, the protection of information resources in multi-user computer systems has become increasingly important. The most common protection measures used in computer system are prevention, detection and recovery [1] [2].

In principle the major part of information systems security strategies are focus on technology with less emphasis on human factor security. As a consequence, since most information systems security strategies are of importance as they concentrate on technically oriented solutions, such as, checklists, risk analysis and assessment techniques, it is important to consider other ways of managing information systems security in light of human factor and related risks within the organizations [3].

This paper focus is on human and organizational factors within organization’s information security system.

Regardless of technical controls, the impact on security can be significant if human and organizational factors influence their employment status and access to secure information resource [4]. As a result, this may trigger computer and information security vulnerabilities that may be set by vulnerable computer and information security protection (e.g., weak passwords or poor usability) in conjunction with the malicious cyber-attacks. Some organizational policies and individual practices of employees within the organization may have significant impact on the system security and [5].

Every organization must review the system security, meet internal and external security standards, and set and enforce the security policies. In order to support proper decisions concerning the investments in security technologies, the organization must establish their own security policies to advice their security professionals, technology officers, financial officers, and organizational managers on how to manage it [6].

Passwords play an important role in daily life in various computing applications like ATM machines, internet ser-
The Secure Role Based Mission System (SRBMS)

Figure 1: The Role Based Access Control (RBAC)

Figure 2: Application Architecture [13]

Access control, or authorization, in its broadest sense has existed as a concept for as long as humans have had assets worth protecting. Guards, gates, and locks have been used since ancient times to limit individuals’ access to valuables. A need for access control in fact prompted the invention of what can be regarded as the world’s first secure computing system [9]. The Role-based access control (RBAC) is most common access control model, and theory and applications are quite common to community of security experts.

The properties of advanced RBAC models, such as the relationship between role activation and permission configuration concerning the interaction between inheritance and constraints are quite complex.

In computer systems security, the RBAC is an approach to set systems access policies to authorized users and to restrict the access to unauthorized users. It is used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC). The RBAC is sometimes referred to as role-based security [10].

The software based RBAC facilitates access to classified resources, keeping the log register and back-tracking the past logins and access to resources by authorized personnel. Within the organization, the roles are assigned by the system administrator accordingly to the user authorization and job functions. The access permissions to perform certain operations are assigned to specific roles following the matrix (Fig. 1). The authorized users are assigned particular roles with authorization to perform particular tasks. Since the users are not assigned permissions directly, but only acquire them through their role (or roles), the management of individual user’s access rights is provided via assignment of appropriate roles to the user’s account. This simplifies common operations, such as adding a user, or changing a user’s department.

Three primary rules are defined for RBAC:

1. Role assignment: A subject can exercise permission only if the subject has selected or been assigned a role.
2. Role authorization: A subject’s active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

3. Permission authorization: A subject can exercise permission only if the permission is authorized for the subject’s active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles. With the concepts of role hierarchy and constraints, one can control RBAC to create or simulate lattice-based access control (LBAC). Thus RBAC can be considered to be a superset of LBAC [11][12].

2. The SRBMS Architecture

The SRMBS was developed utilizing the Spring MVC framework. The SRBMS Architecture illustrated in Fig. 2, consists of the Presentation, Business, Data Access and the Data Store layers. The RBMS architecture consists of the JSP, Spring, Hibernate and Database Systems.

2.1 Presentation Layer

This is the top layer of the application. The presentation tier displays information related to such services as browsing merchandise, purchasing and shopping cart contents. It communicates with other tiers by which it puts out the results to the browser/client tier and all other tiers in the network [13]. In simple terms it is a layer which users can access directly services such as a web page, or an operating system’s GUI. In this upper layer of implemented application, various technologies were used to create a dynamic, responsive and easy to use GUI. The technologies used are listed as below.

- JSTL: JSP Standard Library to make the codes more elegant.
- JQuery: Do less and get more.
- Ajax: Partial rendering page asynchronously.
The Secure Role Based Mission System (SRBMS)

Figure 5: Application Calendar

- JavaScript: ECMAScript to make more friendly GUI
- CSS: Makes the UI look more beautiful.
- Bootstrap: Responsive pages.

The implementation of security components and the SRMBS interface is illustrated in Fig. 3. The user-web interface is shown in the front on the right, showing a dashboard with the user’s access and authentication, geographical location with the specific task assignment.

Figure 4 illustrates selected screen shoot of the application GUI in more details. To illustrate the real case scenario, the left menu lists a Navy Military dashboard, officers’ ranks with their roles, system user, assignments ranks, geographical locations, mission maps, target strategies and new reports. The dashboard provide access to control panel providing statistics reports of a selected assignments accompanied by the mission reports.

In support of control and management of the system, a Fig. 5 illustrates a calendar with the left menu mission specific events and related dates. Each task is highlighted in the calendar showing particular type and dates of the event.

2.2 Business Layer

The business tier consists of components that provide the business logic for an application. Business logic is code that provides functionality to a particular business domain, like the financial industry, or an e-commerce site. In a properly designed enterprise application, the core functionality exists in the business tier components. The controller usually hosts additional logic such as authentication and authorization. It controls which actions a user can execute.

For example, you might not allow a user who hasn’t first logged in to post a message to a message board. If the controller notices that the user is trying to access the “post” page, it redirects the user to a login page first. The user transaction is illustrated in Fig. 6.

2.3 Data Access Layer

A data access layer can be an important part of a software application. Business applications almost always need access to data from relational or object databases and the Java platform offers many techniques for accessing this data, regardless of whether a data access layer is used. The oldest, and most mature and reliable technique, is to use the Java Database Connectivity - JDBC API, which provides the capability to execute SQL queries against a database and then fetch the results, one column at a time.

Although this API provides everything a developer needs to access data and to persist application state, Java Enterprise Edition (JEE) offers a newer persistence framework in the form of Entity Beans, a subset of the Enterprise JavaBean (EJB) framework. Although there have been many improvements in the more recent EJB 2.0 specification, many developers are now looking to alternative persistence frameworks, such as Java Persistence API (JPA).

2.4 Data Store Layer

The need to persist data created at runtime is as old as computing. And the need to
store object-oriented data cropped up when object-oriented programming became pervasive. Currently, most modern, nontrivial applications use an object-oriented paradigm to model application domains. Figure 7, illustrates the Database Design.

In contrast, the database market is more divided. Most database systems use the relational model, but object-based data stores prove indispensable in many applications. Plus, we also have legacy systems that we often need to interface to (Fig. 8).

2.5 Notes about the Spring Framework

The Spring Framework is an open source, lightweight, application framework for development of java enterprise application. The main ideas of Spring Framework were suggested by Rod Johnson, an experienced enterprise Java architect [13]. He had showed the disadvantage of EJB and the traditional approach for development of J2EE application, introduced the concept of Light-weight container through his books Expert One-on-One J2EE.

Spring Framework replaced the complexity of traditional approach for development of J2EE application by adding newer technologies such as Inversion of Control and AOP. This approach helps our development of application to be simpler, easier for test, more effective performance and less cost to develop and maintain. The Spring Web model-view-controller (MVC) framework is designed around a DispatcherServlet that dispatches requests to handlers, with configurable handler mappings, view resolution, locale, time zone and theme resolution as well as support for uploading files [13].

3. Conclusions

The paper illustrated the SRBMS Architecture as a platform to develop a secure role based that could be easily applied for any organization that may conduct a mission critical application such business, government or military. The paper illustrates scenario of a combat-ready naval forces with capabilities to deter any possible cyber security threats.

The RBMS method enables the administrator to add the users and assign for them specific individual roles. Each role has very unique permissions set defined by the RBMS. The RBMS is based on the Role Based Control Access (RBAC). The RBMS creates a platform for the system users to perform various actions based on the scope of their assigned roles.

This paper present a system utilizing a secure access to web applications that authenticate the authorised users based on their roles within the organization. The security features were implemented in all layers of the application. In the presentation layer security was implemented using view level validations. Mainly in the business layer the authors implemented the core part of security of the system, which the role based access control securing access to the database(s).

In future work, we plan develop an information security model for analyzing security. We will also study and characterize standards within the healthcare and government sector.

Acknowledgment

The authors would like to express most sincere gratitude.
to his colleagues from the Department of Computer Science at Maharishi University of Management for their support provided during the course of this work.

References


[15] Everything You Wanted to Know about SQL Injection (But were Afraid to Ask), DZone, http://java.dzone.com/articles/everything-you-wanted-know, access date: 2015. 8. 15.