Improved Access Control Strategy Based on RBAC Model and Its Application

Yin-lei Cheng[1, 2, a*], Fang Wang[2, b], Lei-ming Shang[2, c], Biao-ren Wang[2, d] and Juan Xu[2, e]

[1] School of Computer and Information, Hefei University of Technology, Hefei, Anhui, 230009, China;

[2] Key Laboratory of Neutronics and Radiation Safety, Institute of Nuclear Energy Safety Technology, Chinese Academy of Sciences, Hefei, Anhui, 230031, China

[a]ylcheng2013@mail.hfut.edu.cn, [b]fang.wang@fds.org.cn,

[c]leiming.shang@fds.org.cn,[d]biaoren.wang@fds.org.cn,[e]juan.xu@fds.org.cn

Keywords: access control, MUG-RBAC, CROSSFilter, security framework.

Abstract. System security is a significant factor which focuses on ensuring the reliability and security of system resource. In this paper, a MUG-RBAC (Multistage User Group RBAC) model is proposed based on improved role based access control strategy. The new model increased the entity of multistage user group in the RBAC and fine-grained allocation permissions. The validation of this model is realized in the application to the system security module. CROSSFilter is a part of the informatization platform of collaborative research and management which is developed by INEST CAS for constructing innovative and efficient research environment. By using this model, it shows that the usability of the security module CROSSFilter is enhanced compared with traditional Java security framework Spring Security to guarantee system stability, security and efficiency.

Introduction

With the rapid development of information technology, information-based systems are widely used in many fields. However, due to openness and design defects, some of these systems are vulnerable for attack and information leakage. To ensure system security, a rigorous access control and authority management strategy is required to protect users from hacker invasion and ensure information security. Access control technique [1] is the core technology for informational system security. By identification and authentication, the request for resource access could be managed and controlled. The main existing control strategy includes Discretionary Access Control [2] (DAC), Mandatory Access Control [3] (MAC), Role-Based Access Control [4] [5] (RBAC).

DAC and MAC are improved efficiently by role-based access control model. Different authority is allocated to the roles predefined in the system using access control strategies. The roles connect the access authority with users to make sure they do not connect directly. The user could get corresponding access authority when he gets a certain role. RBAC is the main access control model of informational system for its flexibility, security and convenience. The basic concept of this model was proposed by the security experts in National Institute of Standards and Technology (NIST), since 1990s.In 1996, Professor Sandhu et al put forward the famous RBAC96 model based on the theory, and made further extend on RBAC model in 1997, then put forward ARBAC97 model by using the thoughts of dynamic role management. With the development and application of RBAC.

Recently, RBAC model has been concerned by both the domestic and oversea scholars and research organizations. TRBAC was proposed to describe time character of constraint by introducing time-restriction in [6].TRBDM has been proposed to describing the delegation both static and dynamic separation of duties constraints in [7]. Reference [8] investigated user levels on workflow access control models, designed a method to build a kind of typical user level. The method could be used in RBAC model which supported user levels. Reference [9] proposed a new constrained and distributed RBAC model, defined some concepts such as subject, role, distributed

role, authority, self-organizations, which were used in sharing and serving of distributed remote resources. The research results above provide firm foundation for further research and improvement of the RBAC model. This paper deals with the complexity of the authorized management in system. So a new RBAC model named MUG-RBAC is designed in which multistage user group acted as the core and fine-grained allocation permissions. The models have played a significant role in system. With the fine-grained processing, the model is able to realize easily-operated access-control and reasonable and valid protection in information system resources. Therefore, the model is appropriate for dynamic change of user-group.

In this paper a new optimal design of soccer robot control system which is based on mechanical analyses and calculations on the pressure and transmutation states of chip kick mechanics, this new control system with high precision for speed control and high dynamic quality.

Traditional RBAC

RBAC model provide logical separation of users and permissions by introducing the concept of role. Then, these users could be mapped to one or more roles, which could gain access to system by the corresponding role and thus the user can access the information system. There is a relationship about many-to-many between users and roles in traditional RBAC model. Each user must have one or several roles, and a single role can embody multiple privileges. The relationship between roles and privileges is also many-to-many. People who had access of the system called user. Only a user with authority has access to the system. The user set is represented by Users. Role is an agent layer between User and Permission, which decouples User and Permission relations. In RBAC, Role is used to instead of User and Group to connect the privilege set. Role is commonly defined as a position in the organization. The Role set is represented by Roles. Session is a dynamic concept, and was created by user. In a session, user can activate a set of roles, where a set of roles correspond to a user in system. The session set is represented by Sessions. Permission describes the license for user's access to information system. The Permission set is represented by Perms.

RBAC model makes system security management closer to the reality of application, in which we can easily map the practical management to the security policies. Moreover, RBAC model is flexible to control the whole security policy of the application system, which is helpful for improving the security level of some web applications.

MUG-RBAC

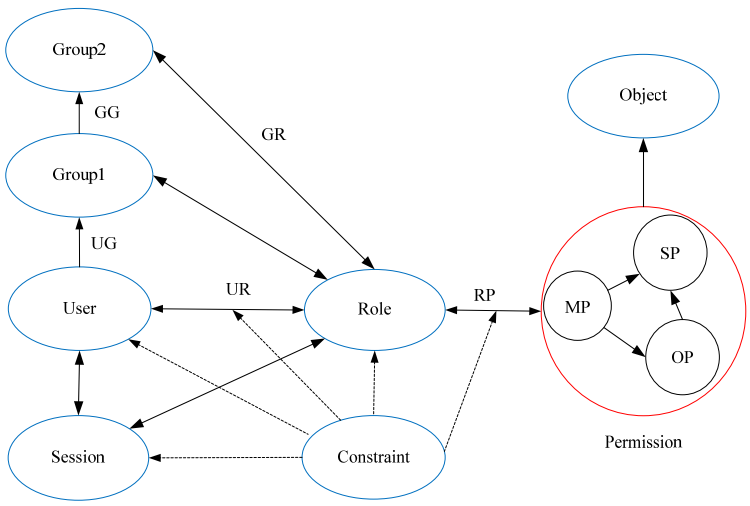

Fig.1. diagram of MUG-RBAC

RBAC model can simplify system and improve the efficiency of organization, enhance the system security and integrity. However, in RBAC model, the original goal is to design the access control of the whole system, which makes the assignment of role-user pair and role-privilege pair much labor intensive. In this paper, a new model called MUG-RBAC, which is based on the

extension of RBAC model is put forward. The MUG-RBAC model inserts more user groups level into the model, make the model more flexible to the application security requirement. The main structure of each element of MUG-RBAC model is showed in Figure 1.

(1)The user Group is tagged Group ($user_1$, $user_2$… $user_n$), composed by a class of common character set classified by user attributes. A user group can be defined as a combination of a plurality of users and other user groups. To define user groups not only need the group name and the description of other relevant information, but also need the parent group except the top user group. The user Group set is represented by Groups.

(2)Object represents system resources, such as page links, database records and files. The object set is represented by Objects.

(3)UR is the many-to-many mapping between Users and Roles.

(4)RH is the many-to-many mapping between Roles and Users, expressed the inherited relation between low and top role, described as: $RH=\{(r_1, r_2)\in RH|(r_1\Rightarrow r_2, r_1、r_2\in Roles) \cap dif(r_1,r_2)\}$ where $dif(r_1,r_2)$ represented both role r_1 and r_2 owned different levels, $r_1\Rightarrow r_2$ expressed Users inherit the access operating authority of Roles.

(5)RP is the many-to-many mapping between Roles and Perms, described as: $RP= \{(r, p, result)\in RP|r\rightarrow p, r\in Roles, p\in Perms\&p= (MP,SP,OP)\}$, symbol $r\rightarrow p$ indicated the permissions p assigned to roles, result indicated the final authorization result as to enable and disable.

(6)Access control is the core framework of the authority in system, the key factor for judging the quality of a rights management framework. In order to meet the needs of practical applications perfect, the MUG-RBAC model is focused on fine-grained divisions, including model permissions, operation permissions and range permissions. The triple array Permission= {MP, OP, SP} is used to indicate permissions. MP is used for determining whether the role has access to a module. OP refers to the operation rights of roles in CRUD of system object. SP refers to the data range of objects in OS of roles. Range permission is used to discriminate the operating range of each role.

User's permission of the module must be judged after the user got the successful landing by verifying. If it existed, then the user got authority of business operating, while giving the corresponding range of rights to the operating authority constraints.

(7)GP is the many-to-many mapping between Groups and Perms, representing the relationship of users' permissions from system.

(8)UP is the many-to-many mapping between Users and Perms.

(9)UG is the many-to-many mapping between Users and Groups.

(10)GR is the many-to-many mapping between Groups and Roles, representing the User permissions inheritance relationship roles.

(11)GG is the many-to-one mapping between one Group and other Group.

(12)Expand-role constraint set is an abstract of constraint on the condition, environment, and restriction of the access. Expand-role constraint set mainly includes features of exclusiveness, dependence, inheritance, cardinality restriction, and containment.

① Exclusiveness means a user can distribute a role of an exclusive role collection at most.

② Dependence means role r_1 should be distributed to a user if the role r_2 is distributed to the user, so call the role r_1 depends on role r_2.

③ Inheritance means if the role r_1 inherits the role r_2, the r_1 will inherit all the restrictions of the r_2.

④ Cardinality restriction means a user can have the role account limited. Besides, the corresponding authority account of a role is limited.

⑤ Containment means if the role r_1 has the containment relationships with the role r_2, so a role has the authority of both the role r_1 and the role r_2.

MUG-RBAC inherits the concept of the role and role control in traditional access control, and increase the entity of multistage user group in the RBAC model. The user group is the collection of the user roles. It is a package of authority of different roles divided according to the attribute of the users. Multistage user group means that it contains a relationship among user groups, department, first group, and second group. It is a collection which is made up of several user groups having a kind of common feature. The top user group is divided according to the attribute of the low user

group. When the administrator allocates more roles to the user, the group can make it easier to allocate the user role and the user in the group has the authority of all the roles in the user group. A user group has several roles and a role can have several user groups. To distribute the roles of the user group is that all users in the group allocate the corresponding authority achieving the effect of batching. Besides, dividing the authority in fine granularity makes the authority of system more accurate. MUG-RBAC makes the RBAC model more flexible in the application, which not only realizes the fine granularity of the RBAC, but also enhances the usability of the management of the authority in system.

The design and implementation of the MUG-RBAC model in the CROSSFilter.

Design process

On the basis of above research, INEST(FDS Team[10]) has designed and implemented an informationization platform of collaborative research and management , called CROSS[11], which aims to simplify the development procedure and improve the efficiency of authority management.

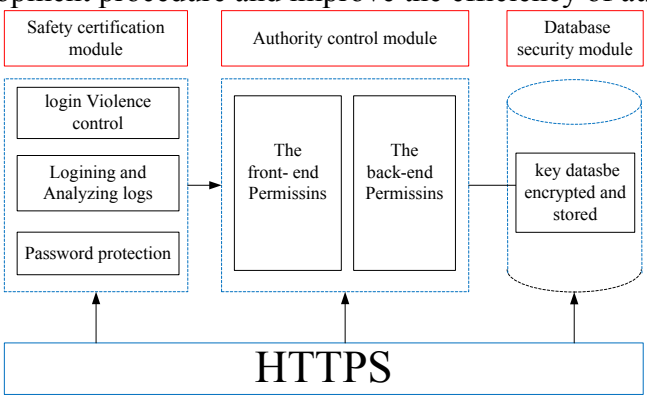

Fig.2. diagram of the CROSSFilter

Figure 2 shows the structure of CROSSFilter, the proposed authority control module based on the MUG-RBAC model. When the user input the url of website in the browser, CROSSFilter will check the identification of the user first and analyze the service request of the authorized user. After the identification authentication, CROSSFilter sends the application request of the corresponding resource to the inner server and to filter the response to the user request. As shown in figure 3, the specific process of CROSSFilter works as follows.

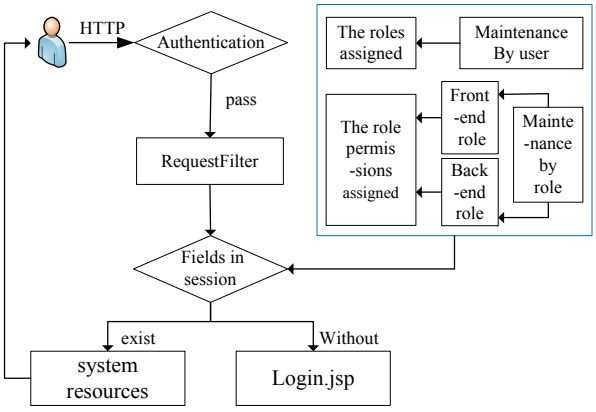

Fig.3. diagram of the process of CROSSFilter works

(1) In access control module, each subsystem corresponds to a web page.

(2)Through a check box in page, system administrators can grant the respective right to the named role. Further, value used a special character @ to separate the front-end permissions tab and back-end permissions tab. The value is divided into two tags by calling a customized function submitted to the database when the administrator saves role authorization.

(3)Use SSO [12] technique to pass the front-end permissions and back-end permissions over to http request session. Therefore, password is no longer needed for resource access.

(4)A global request interceptor is configured in web.xml of the JavaEE application. Meanwhile, a specific RequestFilter which implements HttpServletFilter is configured into the subsystem.

(5)When a user makes a request, the RequestFilter intercepts this request and get the visiting resource link through the request.getRequestURI method.

(6)RequestFilter can assert its rights by calling the checkPrivilege method. If the link of user request is found in the back-tag of the table, the system can allow entry by filterChain and giving user system resources. If the link of user request is not found in the back-tag of the table, some information of user are logged to the log.

(7)In the meantime, if the ashing tag of is not found in the pre-tag of the table, the user can't reach system resources. Conversely, user gets resources and the entire process is finished.

System implementation

In the test, the system supposes that a user visits the page that is not authorized or an illegal user try to access the page after login. In this system, an illegal user is unable to access a protected resource even he successfully by passing the login screen. The system is divided into foreground and background to test the authorized access module. The system guarantees the legitimate operation of authorized users through the foreground restrictions and background control. On the one hand, if a user does not have the permissions, he is unable to gain access to any protected resources through any operations; on the other hand, the string of foreground permissions is used to control user's operations.

In Spring Security [13] framework, the roles, users and permissions are encoded in the xml configuration files and source files. In this way, once a permission is changed, the source code needs to be changed and the service needs to be restarted to read the corresponding access control relationship, which leads to low flexibility for the administrator to control roles. Based on improved RBAC permissions, CROSSFilter security model provides a security maintenance interface include relationships between users, roles and permissions, which achieves the requirements of separation of duty dynamically, and greatly improves the convenience of permissions management. Besides, Spring Security does not provide a good fine-grained permission programs which resulting in maintenance workload and low availability; CROSSFilter successfully achieves fine-grained permissions using the method of separating the labels of front and back.

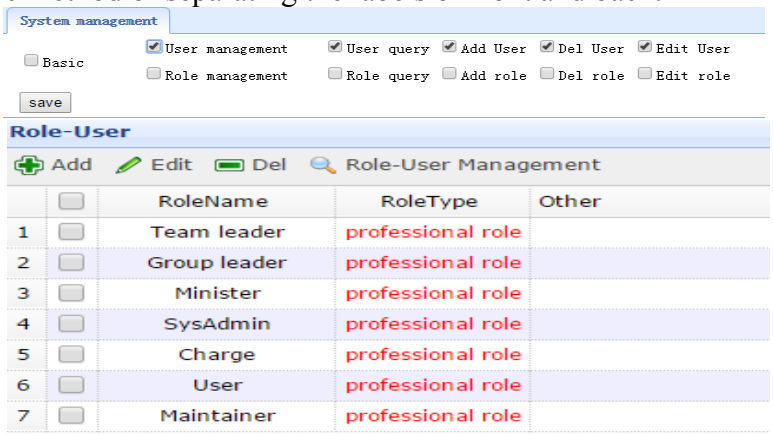

Fig.4. diagram of the implementation of CROSSFilter

Through the above test and analysis, the use of CROSSFilter security architecture significantly enhances the security of important resources in CROSS. Simultaneously the role act is used as a test and analysis bridge between the user and the system, it achieves the dynamic allocation of the fine granularity in user authority, and reduces the license management and the complexity of the maintenance. Figure 4 Shows the implementation of CROSSFilter in CROSS.

Conclusion

With the rapid development of computer networking and enterprise informatization, applications of computer systems in various fields have become more complex. At the same time, there is an increasing demand of the strict management and access control. Through proved RBAC model and

analyzed finely granular access control, this paper sets out design and realization of permission model based on the MUG-RBAC. It not only protects the security of CROSS effectively, but also enhances the usability, extensibility and flexibility of system.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 61202283, No. 61472115), the Special Program for Informatization of the Chinese Academy of Sciences (No.XXH12504-1-09), the Strategic Priority Research Program of Chinese Academy of Sciences (No.XDA03040100), and the Major/Innovative Program of Development Foundation of Hefei Center for Physical Science and Technology. The authors would like to thank the great help from FDS Team.

References

[1] He Bin, Gu jian. RBAC Based Privilege Management Infrastructure [J]. Computer Engineering, 2004, z1(30):326-328.

[2] Department of Defense (DoD) .T rusted Computer System Evaluation C riteria (TCSEC) (DoD5200. 28-S TD 1985). Fort Meade, MD: Department of Defense, 1985

[3] S Osborn.Mandatory access control and role-based access control revisited. In: Proc. the Second ACM Work shop on Role Based Access Control. Virginia: ACM Press, 1997:31~40

[4] D F Ferraiolo, D R Kuhn. Role-based access control [C]. In Proceedings of the 15th National Computer Security Conference. Baltimore, USA, 1992, 08: 554 -563.

[5] R Sandhu, E Coyne, H Feinstein, etal. Role-based access control models [J]. IEEE Computer, 1996, 02, 29(2):38-47.

[6] Bertino E, Bonatti P A, Ferrari E. TRBAC: A temporal role-based access control model [J]. Acm Transactions on Information & System Security, 2001, 4:4-23.

[7] Zhu Jun. Research on Group Awareness and Access Control Technology of Role Cooperation [D]. Guangzhou: Sun Yatsen University, 2009.

[8] R Botha, J Eloff. Designing role hierarchies for access control in workflow systems [C]. In Proceedings of the 25th International Computer Software and Applications Conference on Invigorating Software Development(COMPSAC.01). Washington, DC, USA, IEEE Computer Society, 2001, 10:117-122.

[9] M C Ma, S Woodhead. Constraint-enabled distributed RBAC for subscription-based remote network services [C]. In Proceedings of the Sixth IEEE International Conference on Computer and Information Technology (CIT.06). 2006, 09:01 -06.

[10] Wu Yican, Hu Liqin, Long Pengcheng, etal. Development of Advanced Nuclear Software and Nuclear Informatics [C]. The 3rd China Research Informatization Development Conference. Beijing, CHN, 2013.

[11] Wu Yican, Jia Wei, Wang Fang, etal.The development and application of Informatization Platform for Collaborative Research and Management[J]. Information work dynamics of Chinese Academy of Sciences.2014. 8(50):6-12.

[12] Zhan Jiayou. Security Solution Research In The Single Sign-On [D]. Beijing: Beijing University of Posts and Telecommunications, 2009.

[13] Ding Z F. Access Control for Web Resources Based on Spring Security [J]. Journal of Yichun College, 201