Design of User-Privilege Management in Remote Monitoring System of Radio and TV

Xinglong Liu

College of Information Engineering, Communication University of China, Beijing, 100024, China

liuxlb07@outlook.com

Keywords: user privilege management, database access, monitoring, authentication

Abstract. Radio and television monitoring system is widely adopted by corporations such as transmission monitoring centers and transmitting stations in many provinces. The system is an important technical means to ensure the security of signal transmission and associated facilities. The use privilege management module, an important part of the monitoring system, has significance in protecting the security of transmission and transmitting system of radio and television. However, the problem is that dynamic execution environment constraint and device state constraint have not been considered in authentication and authorization process. In this paper, we introduce a new access control model based on rules constraint especially device status constraint. By establishing custom permission described statements, it can accurately describe fine-grained permission. The simple implementation of the authorization management module is given in the paper.

Introduction

In order to strengthen safety management of broadcast on radio and television, and ensure high-quality broadcast signals, SARFT stipulates the relevant corporations must establish sound technical monitoring system to monitor the main portion of broadcast signals and equipment status, and timely handle broadcast fault. In accordance with this provision, the relevant departments, include transmission monitoring centers, wireless transmitters, broadcasters and cable networks, establish a series comprehensive monitoring system, involving equipment monitoring, channel monitoring, source monitoring, stream monitoring and so on. The remote monitoring and management platform of radio and TV transmission center of certain province has been undertaken by author's laboratory. In this paper, we research and design user-privilege management module of the remote monitoring and control system, combining with the actual situation of radio and TV monitoring and project construction needs. We comprehensively use a variety of right management technologies, with the goal of establishing monitoring and control system meeting the high fine-grained. Our research work includes:

1. Based on the previous analysis about access control model, we propose an authority management model based on rule constraint. Rule constraint includes device status constraints, device relationship constraints, role constraints, time constraints and geographical constraints.
2. Using the thought of rule-based reasoning match as the basis for rights management, we match the current data and the predefined matching constraint rules by introducing rules engine matching constraint rules, and dynamically grant or revoke a user operating authority.
3. Using custom permission expression to describe the operation rights and custom permission expression includes resource domain, operating domain and property domain. We can clearly specify the resource type, allowed operations and accessed data.
4. Using centralized management business rules to achieve a decoupling between business rules and procedures , and to improve the maintenance and reusability of business rules.

Analysis of access control model and rule engine

In this section, we will analyze discretionary access control (DAC) model, mandatory access control (MAC) model, role-based access control (RBAC) model, and task-based access control (TBAC) model. The advantages and the disadvantages of these four models will be compared.

The biggest advantage of DAC model is that DAC has great flexibility. Each entity has a user name and belongs to a specific group. At the same time, each object has an access control list, which is used to restrict access to the main object. Object creator can have access to objects and transfer permissions to others. But many unknown security risks are caused by passing permission with each other. Therefore, the use of this model leads to error-prone.

For MAC model, its core is to set a large number of security levels in system. These security levels include confidentiality and scope. High-level user cannot write data to low-level file, low-level user cannot read the data in the high-level file. The security level cannot be changed by user, and only the system administrator can determine what access permission users and groups have. Because of it cannot be continuously manage authorization, so MAC model is inflexible.

RBAC model is mainly applied static role-permission assignment by giving the role to one user to make user has the role's permissions. When a user becomes a member of a certain type of role, the user can use its operating authority to objects without limit. In assessing the access request, RBAC model does not introduce the contexts of the current task execution as constraints, so it cannot effectively avoid the impact caused by misuse of the monitoring system.

In the monitoring field, TBAC model has some disadvantages on application. In the course of a business process execution, the user successively completes a series of tasks. When he needs to execute tasks which need other users' licenses, the user needs to suspend execution of this process and send permission request message to another user task list. After other users complete the approval tasks, they return authorization request to this user, then this authorized user can continue to perform the task. In consideration of timeliness and complexity of remote monitoring system of radio and TV, TBAC model is not fully applicable to the system.

The model proposed in this paper is mainly based on the dynamic authorization of TBAC. At the same time, a variety of constraints are introduced to dynamically manage the operating authority. The rule engine is an embedded component in the application, which pulls out the business decisions from the application code, uses predefined semantics to write decision logic, receives data input, explains the business rules, and makes decisions based on business rules. Rule engine puts the business data objects and business rules for comparison testing, activate those qualified business rules, and trigger a corresponding operation in accordance with rule execution logic statement. In rule engine, rule base is used to store the rules, and working memory is used to maintain data related to the current state of the execution environment. When business data is inserted into the working memory, it may be modified or deleted. Interpretation of the rules must provide a mechanism to set the priority order of execution for multiple rules. People usually manage the agenda to resolve conflicts between multiple rules. The schematic rules engine is shown in Fig.1.

The reasoning process of rules engine is shown as follows:

1. Input business data into the working memory;
2. Make rules and business data, using pattern matching;
3. Set these rules into the conflict if they conflict with each other;
4. Execute strategy about resolving conflicts. Repeat steps 2-4.

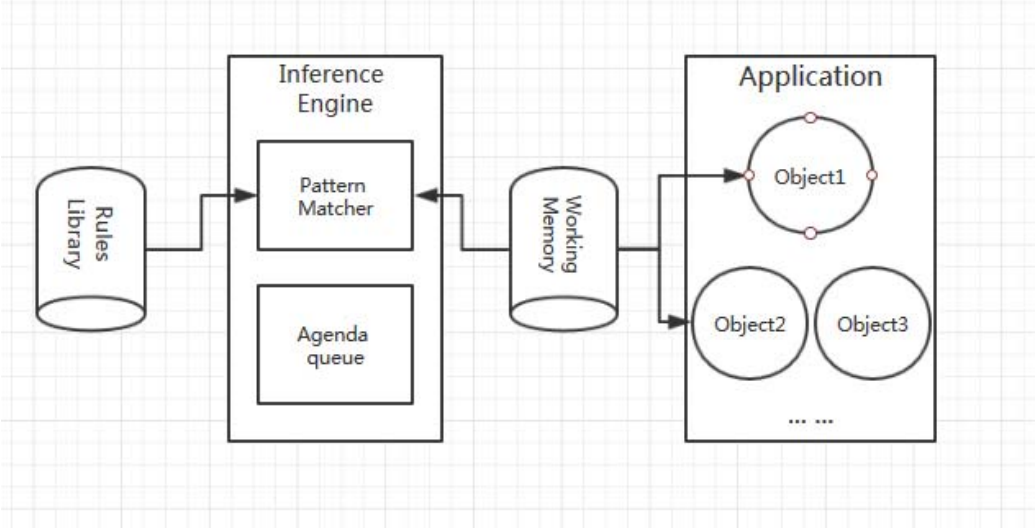

Fig.1 The reasoning process of rules engine

Design of user privilege management module

In this paper, we attempt to use rules engine as the basis for judgment, and judge the conflicts among multiple rules to dynamically update roles-binding permission set in database. When business rules change, we only need to update the rules in the rule files, instead of rewriting the calling monitor. This method greatly increases the flexibility and reusability of software.

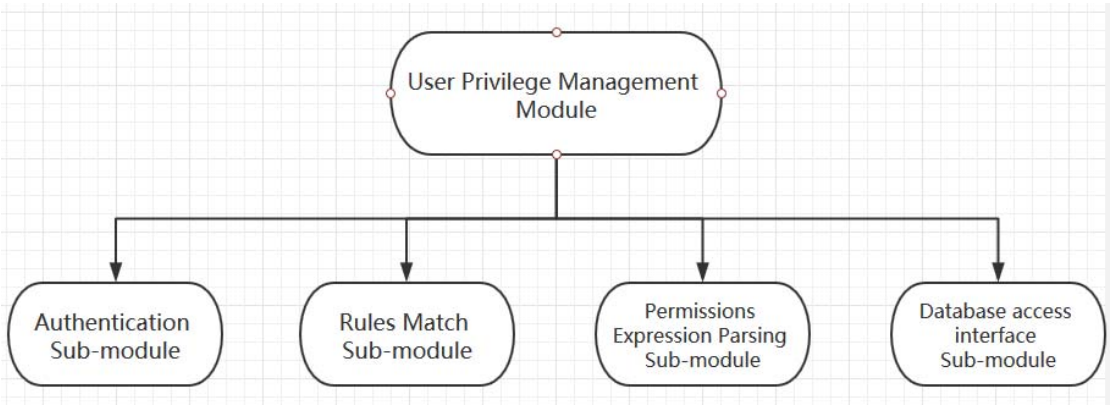

Fig.2 Permissions module overall structure

As shown in Fig.2, the permissions module includes authentication sub-module, rules match sub-module, permissions expression parsing sub-module and database access interface sub-module.

Function of each part is described below:

1. Authentication sub-module is used to verify user identity.

2. The rules engine is used to match runtime data and business rules, and to call the database access interface. The rule-description files store plurality of predefined privilege verification rules.

3. Database Access Service is used to update the role-permission on the table of the database.

4. Permissions expression sub-module is used to explain the custom permissions statement and verify permissions.

Design of authentication sub-module

Authentication is defined to verify the user's identity and user submitted. In most applications, the authentication is completed through a combination of user name and password. In addition, there are other authentication methods, such as fingerprint, certificates, etc. Once one user has successfully

been authenticated, rights management module will take over in order to allow or restrict access. So there is a possibility that one user, who has been authenticated but not authorized, can't do anything.

Authentication module determines the user's roles and basic character attributes through comparing the user name and password information submitted by the user and stored in user table, user roles table, and role permissions table of database. Only authenticated, the user can be able to connect the server of the monitoring system.

The main tables in database include user information table, user roles table, and role permissions table. And the main entities include users, roles, permissions, user-role relations and user-permission relations.

Design of database access interface

The main function of database access interface main is that the interface is called to insert statement that represents role and role permissions into database and to delete assigned role-permission records according to the results of rules match. Generally, common database operations are packaged into a class in the database access service. Simple database access classes are shown in Fig.3.

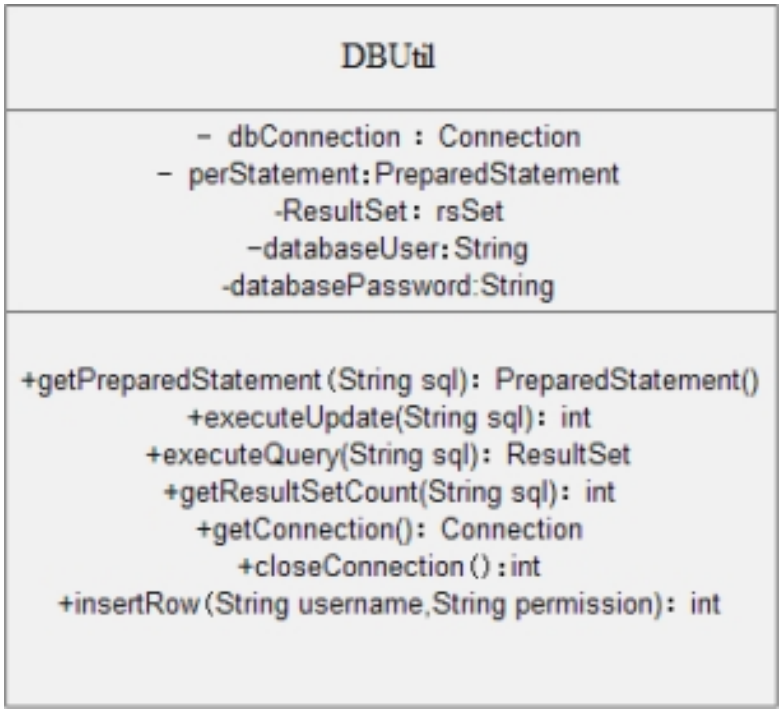

Fig.3 The database access classes

Design of permissions expression parsing sub-module

Permission represents the ability to perform an action or access some resource. For instance, user's viewing a page, using a button, etc. As the smallest unit of the system security policy, permission is the cornerstone of the composition of fine-grained security model. In role-based access control, role represents the behavioral characteristics of certain users. For example, the system includes administrators, users, visitors and other roles. In this dynamic environment, the key is what permissions are given to the role, not the role itself. Permissions in system operation are immutable. By dynamically assigning permissions to roles, users or groups can decides what actions subject can perform to the object. In this way, roles can be created at runtime, configured, or deleted, so that the entire security model becomes more dynamic. We achieve the association of roles and privileges through adding or removing records in the role-permission table.

The abstract of role-permission table is shown in table1.

Table 1 The role-permission table

Id	Role Name	Permission
1	Admin	*：*：*
2	User	Power:read:power01,power02:current
3	User	Transmitter:read,set,open:transmitter01
4	User	UPS:read,open,close:ups01,ups02
5	Guest	Power:read:power01
6	Guest	UPS:read:*

In the role-permission table, one role can be mapped many permissions, also can dynamically insert and delete permission through database access interface after the rule matches. It is notable that, the permission's description is used by custom permission expressions.

Summary

In this paper, we design and implement the access control model based on rule constraint, combining the actual situation of radio and television transmitting station monitors and based on the separation of roles and tasks in RBAC. The model not only meet the principles of separation of functions, least privilege and data abstraction, but also can dynamically validate and assign permissions ,according to the relationship between devices. Thus, system security can be protected to the utmost extent, and dynamic authorization and fine-grained permissions verification can be achieved.

References

[1] Qiu, L., Zhang, Y., Wang, F., Kyung, M., & Mahajan, H. R. (1985). Trusted computer system evaluation criteria. In *National Computer Security Center*.

[2] Thomas, Roshan K., and Ravi S. Sandhu. "Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management." *DBSec* 113 (1997): 166-181.

[3] Giuri, Luigi. "Role-based access control: a natural approach." *Proceedings of the first ACMworkshop on Role-based access control*. ACM, 1996.

[4] Takabi, Hassan, Morteza Amini, and Rasool Jalili. "Separation of duty in role-based access control model through fuzzy relations." *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*. IEEE, 2007.

[5] Grebenik, Vladimir V., and P. Abraham. "Exclusive scope model for role-based access control administration." US, doi:US8255419 B2[P]. 2012.

[6] Wang, Sha, and Z. W. Huang. "Role-Based Access Control." Computer Knowledge & Technology(2007).

[7] Jiao, Xiao Quan, et al. "Design of a New Remote Monitoring System of High-Temperature Industrial TV." Journal of Changzhou University(2013).

[8] Bai, Xiaojun, J. Yang, and Y. U. Jun. "Design of Web-based Centralized Remote Monitoring System for TV Transmitting Station." Video Engineering (2012).

[9] Wang, Hong Yuan, et al. "Remote Monitoring System of High-temperature Industrial TV Based on RF Technology." Control & Instruments in Chemical Industry(2013).

[10] Yao, Gui Ying. "Software Design for Satellite TV signal Monitoring System." Microcomputer Information(2012).

[11] Stephen Dranger, R. H. Sloan, and J. A. Solworth. "The Complexity of Discretionary Access Control.." Lecture Notes in Computer Science (2006):405-420.