Abstract: The Campus Access Network (CAN) is an open network environment in recent years, and presents various users. The CAN security, the security consciousness and skills of people are closely related. Therefore, we must carry through the security education to the different users of CAN, which is beneficial to the CAN security applications. The Role-based Access Control (RBAC) concept and its model are introduced in the paper. The CAN that adopts for designing to specifically access control based on role is also illustrated.

Keywords: CAN; role; access control; security

I. INTRODUCTION

With the increasing development and deepening application of Computer Network Technology, network is penetrating the various fields of scientific, education and economic life. The educational information drives educational modernization, which has become the historical necessity. The information construction at college emerges rapidly as the times just as bamboo shoots in spring after raining. The CAN is an open network environment in recent years, and presents various users. The CAN security, the security consciousness and skills of people are closely related. Therefore, we must carry through the security education to the different users of CAN, which is beneficial to the CAN security applications.

The CAN is divided into two parts: Intranet and Internet. The Intranet as network operation is the busiest and foremost subject, whose security problem seems especially important. If people want the CAN to play a better role, the CAN must guarantee the security of network. The Access Control is an important measure, which controls the accessing range and accessing ability by some methods. The CAN can restrict to access the key resources, and prevent the illegal user from invading or the legal user from causing destroying because of false operation. This paper constructs a access control mould about the internal CAN according to the Role-based Access Control (RBAC) [1-3].

II. THE MODEL OF ROLE-BASED ACCESS CONTROL

The RBAC is a comparatively widely access control strategy in current application, whose core idea is the interrelationship of the access permission and the role. The RBAC distributes the appropriate roles to the user, allows the user and the access permission to relate, thereinto the role is core of the security control strategy. The method of the RBAC introduces the role concept, which realizes the logical separation about the user and permission, thereby makes the permission management get the consumedly convenience. The role can be set according the user in enterprise internal who accomplishes the various different tasks required to arrangement. The user may be endowed different roles. The system may add or delete the role, and roles permission. In this way, the CAN security can be managed by applying the RBAC in a natural platform of similar organization structure [4].

The RBAC generally includes user, role, permission and data object. The relationship of each entity is as follows: The user is initiative side who sends the accessing operation and request, and is the subject that the data object processes operation. The permission is the privilege that a certain data object performs a sort of special operations. The data object is the object of access control, which is usually accessed by calling program or accessing data. The role is an executable and operational set in the system’s user, and is an important concept that is introduced by RBAC. The role is a bridge as contacting the user and the permission. The relationship of the role and the permission may be regarded as that the role possesses a set of the permission, and the association with the user may be looked as the set of users that some possess the same identity. There are multiple relationships among the user, the role and the permission. One user logging in a certain system may judge the system resources which may be accessed and operated by his or her possessing permission of the role. The basic working principle of RBAC is shown in Fig.1.

III. THE DESIGNING PRINCIPLE OF ACCESS CONTROL

A. The principle of mutually exclusive roles

Mutually Exclusive Roles is in order to avoid the one user...
who has both two roles to make potential harm in some cases. The expression of process is integrated with the RBAC on working process designing, establishes direct relation between the task and the role and ensures relevant task communication to be able to guide assignment of the role, sequentially to assure the principle of mutually exclusive roles.

B. The principle of least privilege
The principle of least privilege is when users execute a certain mission, only when users perform the integrant least privilege set of the missions, namely privilege zero redundancy. And only in the course of information flowing, to assure the least privilege, only thus can we ensure the information security.

C. The consistency principle of access control
At present, the management of the CAN basically adopts B/S architecture. When managers make the safety controlling in the foreground, the DBMS of background must make corresponding variety at the same time, to ensure the consistency principle of access control.

IV. THE DESIGNING AND REALIZING OF ACCESS CONTROL

A. The Design Idea
The information system of the CAN is an open system that oriented to multi-application and multi-user, whose information management is much complex. The requirement is relatively higher to data’s safety and security, so we adopt the design idea of RBAC. The system provides much completer setting ability of permission and can set relevant privilege. The system design considers role right code which allows users not only to log on the subsystem, but also to control the user to decentralize the operation to the subsystem for each user [5-6].

B. The Arithmetic Principle
On the design, the system adopts bit mapping to organize the information about function privilege, namely every function privilege is corresponding to a bit. Using “1” stands for permission and “0” stands for forbiddance. These bits that represent function privilege compose binary system, and form the role right code. When the system confirms the current user who is legal user, the system takes out the corresponding role right code of the user, and obtains each function privilege of the user according to the value and specifically mapping relation.

C. The Design of Database
Considering improving query efficiency and reducing data redundancy, we designs five datasheets that is interdependence in the security module of database to store correlated information about users, roles and permissions.

(1) The set sheet of user: USERINFO {User_id, User_password, other user information}
(2) The set sheet of role: ROLEINFO {Role_id, Role_name, other role information}
(3) The set sheet of permission: PERMINFO {Perm_id, Perm_operation}
(4) The mapping sheet of user to role: USERTOROLE {User_id, Role_id}
(5) The mapping sheet of role to permission: ROLETOPERM {Role_id, Perm_id}

D. The Implementation Methods
The security module of RBAC is divided into two parts. One part aims at the user, role and permission of whole information system of the CAN in the set module. In the module, the system can establish new user, and appoint the new user who may log on the authorized subsystem, assign the role in the authorized subsystem for new users, and grant different permissions to diverse roles. The other part sets the module for the user, role and permission of embedding to each subsystem. The establishing new user can only log on the module ubiety of subsystem in the module.

(1) The part of user logon. When users log on every subsystem of the information system of the CAN, they do not allow the unauthorized users to process any operation to the database. While the user input the user account and password, and the user’s information is full true, the user may take out
his privilege code of logging in system and judges the user whether he or she can log on the subsystem or not. When he or she is logging in success, the software module utilizes the role right code to control user decentralization and to operate the subsystem.

(2) **The part of user management.** The part of user management is used to establish new users, maintain the user information, appoint the user to log on the permitted module and assign next role or multi roles of the designation module to the user. The flowing chart of user management of the system is shown in Fig.2.

![Fig.2 The schematic diagram of user management](image)

(3) **The part of role management.** The part of role management is used to found the role of each subsystem, and assign the permission to each role in the system. The assignment of role adopts two methods, namely direct distributing privilege and inheriting the role privilege which has already been in the system.

V. CONCLUSIONS

Role-based on security should be used in two conditions. The first condition is that some portion of the site is restricted to a part of accessing of all users can be accessed by some users. The other condition is that the system wants to know the user’s identity.

The RBAC system researched has many characteristics. The system makes the access control of foreground and background band together, which guarantees the principle of mutually exclusive roles and the principle of least privilege, and is an extremely effective access control mode in the Intranet of the CAN.

REFERENCES