International Journal of Research in Mechanical and Materials Engineering

Journal homepage: http://mcmed.us/journal/ijrmme

AUTHORIZATION MANAGEMENT SYSTEM DESIGN AND IMPLEMENTATION

Xiaoyan Ma*, Zhongdong Han, Hua Ma

School of Information and Engineering, Taishan Medical University, Taian 271016, China.

Corresponding Author:- **Xiaoyan Ma**
E-mail: maxiaoyan81@126.com

Article Info

Received 15/12/2014
Revised 27/12/2014
Accepted 12/01/2015

Key words: Authorization file, Real-time monitoring, Logic design.

ABSTRACT

Authorization management system design is based on .Net Framework platform and Delphi 2006, SQL Server database technology architecture. The operational physical carriers should include: authorization management system, resource management system, and client system. The authorization management system should be designed to realize two functions: (1) Restrict the number of devices and hosts added by clients; (2) Prevent the client to copy the use of system, mainly preventing clients to copy the monitoring management station to multiple computers, and preventing clients to copy the entire monitoring system to other computers.

INTRODUCTION

The real-time monitoring system applied to the power industry is composed of field device status acquisition, background management, storage, configuration, display, analysis and a series of software modules, realizing the functions of telemetry, telecommand, and remote regulation, and truly accomplishing the result of no one on duty.

With the application of real-time monitoring system being more widely, some high-tech users may extend the system into anywhere, or add some devices by themselves for free, after familiarizing the system. In order to protect the system and avoid being copied without authorization, to set up corresponding restriction on the use of monitoring system has become a necessary work.

This authorization management system is designed to strengthen the protection for monitoring system, to make sure that nobody can copy the system secretly without authorization, restrict the final users' implementation scope, and finally achieve the purpose of protecting property right and self-interests.

Authorization management system analysis

`According to the software configuration structure, it can be divided into three parts: authorization management system, resource management system, and client system.

Authorization management system generates authorization file through information encryption and processing.

Resource management system imports authorization files into the data file by certain rules. The number of video and non-video equipments will be limited according to the database file.

Client system is to read, analyze and process the database file through the agreed rules and treatments, and determine whether the module is legitimate software or not. If it is illegal, reject the operation on software functions, otherwise vice versa.

Business process design for authorization management system

Add the field of recording the number restriction to database

Use the data field AddConfig in the SystemData. Data is as follows:

In this table, there is only one record. The field AddConfig contains the registration inforamtion. Resource mangement and monitoring mangement station can read this record for verification.

The AddConfig records data in Json format. To use the Json format can support the continious increase of node contents. The content format is as follows (the actual contents do not contain Spaces and Enters):

```
    {
    "LicenseId":
"2DC7C7B60F694689A4C25BA77FCDFD03",
        //Serial Number Id，used to make comparison
with historical record generated by generator
    "VideoEqs": "1",            //Number of video
equipments
    "NotVideoEqs": "2",         //Number of non-video
equipments
    "Clients": "2",             //Number of clients at
the monitoring station
    "LicenseExpireDate": "21991231"
        //License expiration date, without date limitation,
use 21991231, only for resource manager restricting data
increases
    "LicenseGenDate": "20131216"
        //License generation data
    "ServerName": "Clu"                   //Server name
    "HashCode": "ABE0FA",                 //Abstract
Hash value
    "TempLicense": "1",         //Whether it is
temporary license; when temporary license happens, add
this information
    }
```

Number record prevents unauthorized changes

In order to prevent unauthorized changes of database contents, use the following measures to achieve the purpose.

HashCode generation: Delete the invisible characters (Spaces and Enters) and the left brace from the previous version of “HashCode”, and replace the comma with REALTIME. Then, compute two times of md5. Compare the newly- generated visible text with the HashCode value. If consistent, it means not being modified.

1) Take the full text

```
{"LicenseId":"2DC7C7B60F694689A4C25BA77FC
DFD03","VideoEqs":"1","NotVideoEqs":"2","Clients":"2"
,"LicenseExpireDate":"21991231","LicenseGenDate":"201
31216","ServerName":"Clu","HashCode":"ABE0FA","Te
mpLicense":"1"}
```

2) Delete the invisible characters (Spaces and Enters) and the left brace from the previous version of “HashCode”, and replace the comma with REALTIME.

```
"LicenseId":"2DC7C7B60F694689A4C25BA77FCD
FD03"REALTIME"VideoEqs":"1"REALTIME"NotVideo
Eqs":"2"REALTIME"Clients":"2"REALTIME"LicenseEx
pireDate":"21991231"REALTIME"LicenseGenDate":"201
31216"REALTIME"ServerName":"Clu"REALTIME
```

3) Computing md5

```
HashCode                                          =
md5(md5("LicenseId":"2DC7C7B60F694689A4C25BA77
FCDFD03"REALTIME"VideoEqs":"1"REALTIME"NotV
ideoEqs":"2"REALTIME"Clients":"2"REALTIME"Licens
eExpireDate":"21991231"REALTIME"LicenseGenDate":"
20131216"REALTIME"ServerName":"Clu"REALTIME))
```

4) Determine whether the calculation result is consistent with the content of “HashCode” field.

HashCode verification needs to be based on monitoring management station and resource manager. After the software module above read the data record, it makes verification of the data. If correct, the software operates normally; if not, warn the user “incomplete or incorrect license information monitoring system” and exit.

The number of common equipments and the number of video equipments allowed by resource management

Resource manager reads the registration information stored in database and records the number of common equipments and the number of video equipments in the registration information. When the user increases Configuration ->select a template, judge whether it is a common equipment or video equipment, and respectively evaluate the existing numbers. If the existing number >=the restrict number, warn the user “exceed the system-allowed maximum, please contact the manufacturer to obtain the authorization for more equipments”.

Add the data of recording the information of the login clients

Add the ClientLoginInfo to record the login information of clients. The structure is as follows:

This table does not distinguish CS client from BS client. To log in CS client or BS client in the same computer will be only recorded once in this table.

Restrict the number of login on the client monitoring management station of the system

The CS monitoring management station and BS Web server need to judge whether the number of clients exceeds the limit.

When CS monitoring management station logs in one computer, it must list all IP addresses of the computer. Compare these IP addresses with the database IP address. Authorize the forward highly-matching IP address as the IP address.

When BS Web server monitors a login request from a client, it obtains the IP address of the client computer and takes it as the authorized IP address.

Comparing the authorized IP address with the ClientLoginInfo record in the database, if exist, allow the login; if not exist, calculate the number of records in ClientLoginInfo. If the number>=the restricted number of the registration information, forbid the login; if the number <the restricted number of the registration information, add the authorized IP to the database and allow the login.

The common login needs to update the information in ClientLoginInfo, include:

```
    LastLoginTime = now
    LastLoginType = 0/1
    LoginCount += 1
```

Generate authorization file by encryption

With the application of user, company officials generate the registration file, namely the authorization file, for the field personnel. It contains the authorization information. In order to prevent against forgery information, the server encrypts the information by public key and sends back to the client. The client decrypts the information through the private key.

In this system: The authority system (the server, a controlling software module in the company) generates a pair of keys, using the public key for encryption and keeping the public key secret. After the authority system receives the authorization file, it uses the pre-set private to decrypt the information and gets the authorization file. During the whole process, the private is hidden in the client side, no necessary to keep secret.

Use the RSA to encrypt the authorization file. The contents of the authorization file are as follows:

```
    {"LicenseId":"2DC7C7B60F694689A4C25BA77FC
DFD03","VideoEqs":"1","NotVideoEqs":"2","Clients":"2"
,"LicenseExpireDate":"21991231","LicenseGenDate":"201
31216"}
```

Prevent reuse of registration information

To prevent users from reusing the registration information, once the registration information is input into the system, the server name will be recorded into the registration information. If you want to avoid reuse of the registration information, this information field needs to be added to the Hash section.

For the case of a cluster, we can get the SQL server name through SQL statement:

```
    select serverproperty('MachineName');
```

Import the authorization file

When importing the authorization file, the private key needs to be used for decryption. Then, check on the expiration date. If expired already, no permission for import; if not expired, import the information into database.

If there is AddConfig record in the database, update this record. But before the updating, warn the user about the differences between the existing registration information and the new registration information and wait for the user's confirmation. If there is no record, insert a record and save the registration information.

Nonproliferation for authorization file generation program

Authorization system is responsible for the generation of authorization file. To prevent the authorization system is freely distributed, we should use the authorization system, the same as existing resource manager, and combine it with local resources. After the combination, copying will not achieve the generation of authorization file. The certification of authorization system needs the participation of personnel from development department.

Clear up the number of once-operated monitoring stations

The user can choose to clear up all login record information of monitoring station. It clears up the ClientLoginInfo table.

Initial installation treatment

The resource manager checks for the initial installation. When resource manager's judge data list CombInfo is blank and the field AddConfig is blank, we regard it as the initial installation.

Once taking it as the initial installation, it generates a temporary authorization file, which allows 10 video equipments to be added, 20 non-video equipments, and 3 clients. Mark the "TempLicense" with "1" in AddConfig. It means this data is temporary authorization.

Once the resource manager starts, it reads "TempLicense": "1". If exist, warn the user "you are currently using a temporary authorization, please contact the manufacturer to obtain the official authorization file. \n The temporary authorization allows only a small amount of data increases and restricts the number of running monitoring stations.

The treatment after upgrading

The resource manager determines whether it is the upgraded state. When the resource manager determines that the CombInfo is not blank, but AddConfig is, it is the upgraded state.

After the resource manager makes the judgment of upgraded state, it generates a temporary authorization file, which allows to add more 20 video equipments, 50 non-video equipments, and 10 clients. It marks the "TempLicense": "1" of AddConfig, referring to the data as temporary authorization.

After starting the resource manager, it reads "TempLicense": "1". If exist, remind the contemporary authorization.

Implementation of authorization management system

The authorization generator interface includes two functions, i.e. configuration of authorization numbers and configuration of authorization information. The user can import relevant information as needed.

Configuration of authorization numbers:

The number of authorized video equipments: The user inputs the number of video equipments into the text box.

The number of authorized non-video equipments: The user inputs the number of non-video equipments into the text box.

The number of authorized clients at monitoring station: The user inputs the number of authorized clients into the text box.

The customer receiving the authorization: Input the name of the customer.

The location to save the authorization file: Click the “ 💾 ” icon and select the location from the pop-up selection box to save the authorization file.

Authorization generator interface

The import interface for authorization file

Open the import interface for authorization file. For the initial installation, the interface will show the “temporary authorization” information. After importing the authorization file, the “temporary authorization”, attached behind the “authorized information”, will disappear from the interface.

The clear-up interface for client login information

The authorization file sets restrictions on the number of logged-in clients. When the number reaches the maximum, the user can delete all login information through the clear-up function and log in again.

The user can read the information of logged-in clients at the monitoring station from the interface. Click the “Clear the client login information”, and the system will delete the information recording the clients logging in monitoring station. Click the “Close” icon, and the interface will be removed.

Table 1. Authorization Management Module Menu

Authorization managementsystem	Support the self-defined video equipments, non-video equipments, and the number of clients
	This system is combined with the computer, invalid for any copy or distribution activity.
	Support for defining the save location of authorization files.
	Support the generation of authorization file.
	Support the authorization generation logs.
	Authorization files are stored by means of asymmetric encryption.

Table 2. Resource Management Menu

Resource management system	Support the import of encrypted authorization file.
	After importing authorization file, combine it with the server.
	Impose check restriction on users adding video equipment.
	Impose check restriction on users adding non-video equipment.
	Reject the import of invalid authorization file.
	Use the hashing algorithm to avoid users modifying authorized contents.
	If the authorization information is blank, the system generates the temporary authorization automatically.
	Warn users about the temporary authorization at the enablement.
	Verify the authorization information after enablement.
	Allow to clear up the logged-in client list.

Table 3. Client System Function Menu

Client system	Verify the accuracy of authorization file when user logs in.
	Report the logging information to the system.
	Check whether the number of logged-in clients exceeds the restriction.

Table 4. Data filed of database

Column Name	Data Type	Data	Description
AddConfig	nvarchar(max)	{"VideoEqs": "1", "NotVideoEqs": "2", "Clients": "2", "ServerName": "Clu" "HashCode": "ABE0FA",}	The extended attribute of Json format is used to save the display of extended attributes. It does not support arrays, or nests, but only support the string type.

DISCUSSION AND CONCLUSION

Firstly, analyze the functions of the three modules of the system and identify the specific needs of every function. Secondly, design the program based on the function. Finally, implement the system functions according to the detailed design. The design of this authorization management system can strengthen the protection for monitoring system, restricting the application of end users. Nobody can copy or use the monitoring system without authorization.

REFERENCES

1. Wang, Xueqing. (2003). Delphi 6 Database Design Examples Navigation [M]. Beijing: The Science Press.
2. Zhang, Yousheng. (2005). System Analysis and Design Technology [M]. Beijing: Tsinghua University Press, Mar.
3. Fu, Jun. (2005). Delphi 7 Programming Examples 100 Cases [M]. Beijing: China Railway Publishing House.
4. Huang, Tiyun. (1985). Introduction to Management Information Systems [M]. Beijing: China Machine Press.
5. Zheng, Ronggui. Huang, Ping. Gu, Huidong. (2002). Delphi 6.0 Database Development and Application [M]. Beijing: Beijing Hope Electronic Press.