Design and Implementation of Encryption Scheme in Web-based Examination System

LI Yong-fei
Department of Computer
North China Institute of Science and Technology
Beijing, China
lyf518@ncist.edu.cn

***Abstract*—Requirements on encryption of web-based examination system were analyze, and different encryption technologies were used to meet the needs on three levels, including important data, core processing logic and some restricted functions. For important data, its confidentiality and integrity were realized. The core processing logic in ASP script was built in COM component. And some restricted functions were protected with hardware key. Encryption which protected data, code and function provided necessary safety for the web-based examination system.**

Keywords-web-based examination; data encryption; COM component; three-level encryption

I. INTRODUCTION

Web-based examination system had been widely used in a variety of education and training assessment. It provided such functions as selecting questions randomly, automatic grading and examination file management. There were some special requirements in impartiality, confidentiality and authorization forms for the web-based examination system used in the field of industry certification. These encryption requirements were analyzed and solutions and implementations were proposed.

II. ENCRYPTION REQUIREMENTS OF WEB-BASED EXAMINATION SYSTEM

A. Architecture of Web-based Examination System

The web-based examination system mentioned in this paper was used for a particular industry certification.

The software used a combination of Browser/Server mode and Client/Server mode. Browser/Server mode was used for online examination and Client/Sever mode for examination management. The software was installed in the computer lab of the training institutions with assessment qualification, running in LAN.

The architecture of web-based examination system was shown in Figure 1.

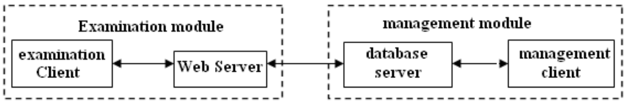

Figure 1. Architecture of web-based examination system

B. Encryption Requirements Analysis

The examination system was running on the database management system in user’s computer. Thus the encryption requirements were mainly to prevent user’s directly manipulate the database through their database management system. Detailed Encryption requirements were analyzed as follows:

- Encryption protection for exam score. The score was generated by the rating code in software and stored in database as field values. So it must be protected to avoid man-made changing. The man-made changing may come from three illegal operations: directly modify the value of score field through the database management system; modify the value of student name to change the examination result indirectly; and modify the rating code to save arbitrary value for score field. The three illegal operations must be prohibited by encryption, called respectively requirement1-1, requirement1-2 and requirement1-3.
- Encryption protection for exam question. All exam questions were stored in the database, and the end user could be obtained the electronic version of the questions. For copyright of the questions, it should be encrypted, which was called requirement2.
- Encryption protection for Login password. User with Different identity had different administrative privileges, which be achieved by user name with login password. Login password protection consists of two aspects: First, put an end to view password fields directly through the database management system (requirentes3-1); two, refused to obtain unauthorized privileges by modify the password field value through the database management system (requirement3-2).
- Encryption protection for exam function. As used for an industry qualification examination, the examination system should be authorized to use by the industry administrative department. So the exam function need to be encrypted, and could be used only by the authorized examination institutions (requirement4).

In conclusion, there were 6 requirements of encryption for the examination system.

Published by Atlantis Press, Paris, France.

III. Design of Encryption scheme

Based on the Analysis of encryption requirements, the encryption scheme should contain four aspects:

A. Data Integrity

Data integrity [1] defined in Cryptography referred to that the message recipient could verify that the message had not been modified in transmission. We borrowed the concept to represent that the database field value had not been changed illegally. The requirement1-1, 1-2, and 3-2 were all data integrity requirements.

B. Database Security

Database security was important in the database's data protection. For web-based examination system, database security is mainly reflected in the encryption of field value. The requirement2 and requirement3-1 were all database security requirements.

C. Forbidden to Modify Code

Requirement1-3 was the requirement for forbidden to modify code. Due to the limitations of the ASP technology, the rating code and database connection information in the software were scripts in plaintext. It's necessary to package and hidden them to avoid maliciously tamper code for exam cheating by software users.

D. Restrict the Use of some Functions

Requirement 4 was about the restriction of some functions of the software. That is, the exam function could be used only with the permission in some form from the industrial administrative department. Other functions could be used without permission.

IV. Implementation of the encryption scheme

The designed encryption scheme was realized on three levels: data level, code level and application level, as shown in Figure 2.

A. Data Level Implementation

- Integrity protection. The integrity of the student information was to avoid the user to directly modify the value of score field or student name field in the database management system. The trigger [3] in DBMS was used for the fields which need to be protected. The trigger condition was the change of field value. When the trigger was running, it would check a special tag field. Only when the value of the tag field was a specified one, the change was allowed. And the initial value of the tag field was set to an illegal value. Thus when the user directly modified the field value, it would be rejected due to the illegal value of tag field. The software would modify the tag filed value to the specified one and then go to change the protected field value, and finally modify the tag field value to illegal. A simple integrity protection was implemented in the way.
- Question encryption. XOR encryption algorithm was used to encrypt all questions, and then stored into the database and distributed to end-users with the software. As long as the encryption key was confidential, the confidentiality of the questions would be well implemented. In examination, the encrypted question was extracted from the database and decrypted. XOR encryption algorithm was selected mainly because it's relatively simplicity. In examination, if the encryption algorithm was too complicated, assembling paper with decrypted question would be so slow that affect the software response speed.

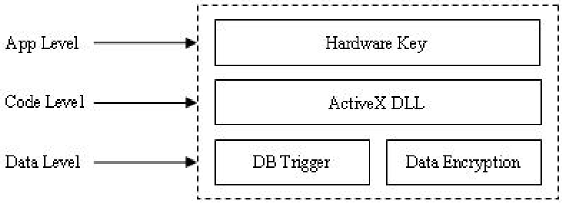

Figure 2. Encryption Scheme on multiple levels

- Password encryption. Login password was encrypted with MD5 algorithm, which was one-way encryption protection. Thus user could only see the MD5 cipher text of password to avoid disclosure. When user login, the software encrypt the password entered by user and compared the result with the cipher text stored in database.

B. Code Level Implementation

There was some core business logic that was not suitable for storing in plain text. These core business logic included rating code, database connecting code and question decryption code as well as the code that modify tag filed value to avoid trigger protection. All these core code were packaged in a server-side component by the means of ActiveX DLL. And the plain text code was transferred to binary code identical with ordinary PE file. The encapsulation of core code was effectively achieved [4].

C. Application Level Implementation

Restriction on the use of software function was to encrypt exam function in application level, so that the user must have permission to use it. There were two kinds of application level implementation, software encryption and hardware encryption.

Software encryption referred to that user must enter a special password to run the function. The disadvantage of this encryption was the password was easy to leak. Once the password was stolen by others, the encryption effect was lost. Hardware encryption referred to that user must insert an encryption device into a specified port, and could use the function only after validation. The hardware encryption was much safer and more intuitive than software. And it visually represented the authorization by administrative department. So, a hardware key was used for application level encryption.

Published by Atlantis Press, Paris, France.

V. SUMMARY

In this paper, the encryption requirements were analyzed, and various encryption technologies were selected to build a multi-level encryption scheme. The Given scheme had been applied in a web-based examination system, and a good effect had been achieved.

REFERENCES

[1] Shen Xin-yan, Computer Network Security. Beijing: Tsinghua University Press, 2009(in Chinese) .

[2] Chen Yue, Database Security. Beijing: National Defense Industry Press, 2011(in Chinese).

[3] Jiang Gui-hong, SQL SERVER 2005 Database Application and Development. Beijing: Tsinghua University Press, 2010(in Chinese).

[4] Zheng Yu, Yang Chun-sheng and Yu Jiang. Encryption and Decryption Combat. Beijing: Electronic Industry Press, 2006(in Chinese).

[5] Deng Jian-gao and Pan Jiang-bo, “Research on Security of Web Database based on Java2 Security Architecture”, Computer Engineering and Design, Nov. 2007, pp:2739-2741(in Chinese).

[6] Guo qiang and Lu Shu-wang, “Study on Security of Bidding Website”, Computer Engineering and Design, Feb. 2007, p:320-321, 357(in Chinese).