Campus Card System Protection Design Based on Encryption Technology

Huijie Zhu[1,a], Chunbo Wei[1,b], Guotao Xu[1,c] and Lan Luan[1,d]

[1]Hunnan Road, Hunnan District, Shenyang City, Liaoning Province, Shenyang Jianzhu University

[a]zhuhuijie9990@163.com,[b]weichb@sjzu.edu.cn,[c]2670787599@qq.com,[d]854128356@qq.com

Keywords: Encryption, Campus card, Information system, Design

Abstract. Objective: This paper describes in detail the design of campus card system protection system based on encryption technology. Methods: The design and implementation of the server-side management-side management module, rights management module, communication module, and log management module are described in detail design, application of key technologies, and specific implementation aspects. RESULTS: A set of theory and design schemes for security fire prevention of campus card systems based on encryption technology was proposed. Conclusion: Applying the techniques proposed in this paper can effectively improve the level and level of security protection for campus card systems and provide support for information security protection.

Background

With the rapid development of science and technology, the technologies and products that can be applied to the campus card system are endless[1]. The systems and products used in the project should enable users to benefit from it. However, with the increasingly widespread application of campus card systems, the scope of information exchange and resource sharing involved is also expanding[2]. There are many businesses involving personal cash assets. Therefore, the subsequent security problems have become increasingly prominent[3]. Looking at the development trend of college campus card systems, we can see that the campus card system has already involved all aspects of colleges and universities. The campus card system occupies an important position, and once the system security problems occur, it will bring serious consequences[4]. Only if its security is guaranteed can it ensure the smooth progress of work and life in colleges and universities. In general, college campus card systems include the following systems: consumer systems, access control systems, parking systems, attendance systems, and patrol systems. In these systems, the consumer system is directly tied to the funds. The attendance system is connected to the employees' wages in many colleges and universities[5]. The access control, parking system, and patrol system are important barriers to ensure the safety of colleges and universities.

In particular, through the information connection with other management system modules, the entire university network is organically and efficiently brought into motion, making the work of colleges and universities in all aspects smoother due to the high efficiency and simplicity of the CPU card. The college campus card system as the core module of the intelligent university construction is not only the subsystem system of the campus card system, but also combined with various management information systems of colleges and universities to provide a cross-platform, cross-database self-developing information platform. The security issue is even more important. If there are flaws in management, there will be a phenomenon that “smears of fire in cities and gates will catch fire”. This is an opportunity for criminals who steal confidential business secrets from universities and intend to disturb the normal work of colleges and universities. Therefore, how to effectively use the campus card system to bring convenience to university staff and at the same time prevent core secrets from being leaked out by malicious people becomes a research topic that is increasingly concerned about the security of campus card systems.

Encryption Technology

The encryption technology in network security is the basic and important part. Data encryption

technology refers to transforming an information or plaintext into a ciphertext by an encryption function or an encryption key, and transmitting it on a public network. The receiver then transforms with the corresponding decryption function, or decrypts it with the decryption key, turning it into plaintext[6].

To prevent the leakage of information, it should be ensured that only certain legitimate users can receive legitimate data on a specific network, and that these data can be restored to obtain the original data[7]. So the key is to guarantee this situation, this is the role of the key. The key types are generally divided into three types:

Private key: Symmetric and single keys are private keys. As the name implies, it means that this encryption method only uses the same key and algorithm. Such as DES. This method is relatively simple. After the sender uses this key for encryption, the receiving user can decrypt it with the key he gave. For example, an encrypted document is transmitted after being encrypted by a key, and the original data can be obtained after being decrypted by the same method.

Symmetric key: The symmetric key was generated very early, because symmetric keys have the characteristics of small computational speed, high speed, and high security, so many people use it. The entry parameters of the DES algorithm are as follows: Data, Key, Mode. Among them, Data is 8-byte 64-bit, which is the data to be encrypted or decrypted. The key Key is the working key of the DES algorithm, which is a total of 64 bits; Mode is the working mode of the DES, and there are two types: encryption or decryption.

Public keys: Public keys can also be called asymmetric keys, and different keys are used for encryption and decryption. It is impossible to easily derive one from the other, but there is a certain relationship between the two. Like the RSA algorithm, a public encryption key is encrypted and can be decrypted with multiple decryption keys. The relationship between these two keys is basically a mathematical logical relationship. Both the public and private keys are a set of mathematically logically related long prime numbers. Because a message encrypted with one key can only be decrypted with another key, there is one key that is insufficient to translate the content of the message. A user has only one pair of keys, one is a public key, and the other is a private key. The public key can be placed in a common area and can be delivered using a network or storage medium. The private key should be stored in a safe place. The working process of encryption and decryption can be understood as: first encrypt the file with the public key, which can prevent other people from monitoring, but only the personal private key can decrypt the information, so that the information can not be disclosed. The public key has better confidentiality, so long as it has a public key, it can send a document. Digital signatures use a method of authentication that can prevent falsification.

Asymmetric encryption technology: For example, RSA, digital signatures generally use asymmetric encryption technology, and the results of transforming plaintext are used to verify the signature. The recipient uses the sender's public key to decrypt the operation. If the obtained result can be converted into plaintext, then the authenticity of the sender's identity can be proved. Signing can also be done in a variety of ways. Digital signatures are commonly used in e-commerce and banking. Digital signatures are different from handwritten signatures. Handwritten signatures reflect the characteristics of a person and are therefore not easily changed, and digital signatures change as the text changes. Textual information and digital signatures are integrated, but handwritten signatures are signed after the text and are not related to the text itself[8].

Campus Card System Protection Design based on Encryption Technology

The entire campus card system consists of three parts: the data center, the server, and the client.

The system data center runs the database operating system, storage rights strategy, encrypted system data, permission tables, and other background data information that provides support for the entire system operation. According to the classification of data information, the database establishes a user information table, a CPU card information table, a management side information table, a permission classification table, a department information table, a sub-table of each subsystem, a log record table, a role information table, and a DES key table. Ten data sheets. The initial campus card system comes with a server-side security management module. The security management module

provides a high-performance security solution for each subsystem. The secret-pin interface enables convenient access to the system to be stable and safe. The security management module is the basic module of the entire system, and is also the management strategy highlighted in this paper. It is divided into several parts according to the function of the module, including: central management module, personnel management module, card management module, management-side management module, transmission management module , permission configuration module, log management module.

The client includes various subsystems such as access control and consumption. The campus card system includes a wealth of systems that can be tailored to project customization needs. Choose among different projects and guarantee stable operation. Each submodule must exchange information with the communication module, and data exchange is performed at the data exchange layer. Such as encryption and decryption and primary data processing, will be completed within the communication module. The communication module supports common protocol methods such as Modbus, and also supports the custom communication protocol that comes with the system. After the communication data is processed, it will be returned to the upper layer via the TCP/TP method, that is, the server. The server structure is complex, including the central management module, rights management module, log management module, transmission configuration module, encryption module, and personnel management module. At this level, the key module is the central management module, which includes the upper management of all subsystems. But the central management module

The security guarantees are provided by the surrounding modules. First of all, before logging on the system, the dongle verification is performed. After the verification, the user's login permission verification is performed. For non-privileged users, the module is locked. The transmission management module included in the central management module performs security management on the transmitted data. For example, data security configuration can be performed, including whether encryption is performed or not, and in what manner encryption is used. The central management module also includes card management, and the card is issued by a secret management system, which protects the uniqueness of the card password. All data is centrally stored in the data center.

Management side management module: The management side is a collection of management modules responsible for all subsystems. It integrates multiple systems such as access control and time attendance into a whole, and manages all personnel data and card data. Including personnel, cards, role assignments and other modules. The management end module is an important part of the campus card system. The core data is the same as the management and configuration of the module. For the management side management module, there are two security measures: login verification and dongle verification.

Rights management module: The rights management module mainly manages the data related to the operation authority of the subsystem. Used to maintain the database's rights management table, to achieve the allocation of user permissions for each subsystem and related department permissions.

Communication module: The communication module type is an important part of the security protection system. The data communication protocol Data Communication Protocol can also be called data communication control protocol. It is mainly a series of agreements stipulated in order to ensure that communication parties in a data communication network can be effective and then complete reliable communications. These conventions include the format of the data, confirmation or rejection of data transmission, sequence and rate, error detection, retransmission control, and interrogation operations.

There are two types of data communication protocols: one is the basic type of communication control protocol, which is mainly used for data transmission based on characters as the basic unit, such as the BSC protocol; the second type is called the high-level link control protocol ALCP. Bit-based data transmission, such as advanced data link control protocol and synchronous data link control protocol. The basic protocol is used in a simple low-speed communication system, and the communication mode is generally an asynchronous synchronous half-duplex mode. Error control is

a policy code verification. The high-level link control protocol generally adopts the unified format. Because of its high efficiency, it can be widely used in public data networks and computer networks. Different workstations in the network can transmit data between servers because of the existence of protocols. With the development of the network, different operators have developed different communication methods. To make communications more reliable, all hosts on the network must use the same language and cannot have special languages. So a strict standard must be developed to define each bit in every word in every packet between hosts. All of these standards come from the efforts of multiple organizations, and agree on a common communication method. This is the agreement. The protocol can make communication easier. This article uses a custom communication protocol to ensure the security of the system and prevent it from being easily cracked.

The communication module is responsible for delivering the commands of the management terminal to each client and receiving the returned data of the client to the upper management terminal. In practical applications, there will be more specific effects. For example, in a consumer system, it is responsible for transmitting all consumption data, white lists, consumption types, and the like. In the access control software, credit card data, personnel data, and alarm data of the access control are transmitted.

The communication module uses a custom interactive protocol to ensure that if the data is intercepted and leaked, the real data cannot be illegally tampered to ensure data security. The protocol definition mode is: command, length, data, verification, and the client's communication module is matched.

Summary

This article describes in detail the design of campus card system protection system based on encryption technology. The design and implementation of the server-side management-side management module, the rights management module, the communication module, and the log management module are described in terms of detailed design, application key technologies, and specific implementation aspects; the client part first introduces the client-side architecture design, and then, The communication management module, the card verification module and the client legal verification module are described from three aspects: detailed design, application of key technologies and implementation.

References

[1] Mitsuo Usami.An ultra Small RFID chip: μ-chip.In Asia-pacific conference on advanced System Integrated Circuits-AP-ASIC 2010:2-5

[2] T.Staake, F.thiesse, and E.Fleisch, Extending the EPC network: The Protential of REID in anti-counterfeiting , 20th ACM Symp, On Applied Computing ,santafem.NM,2005:1607-1612

[3] Suhaiza Zailani,Liu Wen Sze,Yudi Fernando.Determinants of RFID Adoption in Supply Chain among Manufacturing Companies in China: A Discriminant Analysis. Journal of Technology Management & Innovation . 2017

[4] Y.L.Alain,T.S. Chan. Structural equation modeling for multi-stage analysis on Radio Frequency Identification (RFID) diffusion in the health care industry. Expert Systems With Applications .2017 (10):62-67

[5] I.A.ALMERHAG.Key Length as a Qos routing metric. Woodward M E. Sixth Informatics Workshop.2005: 233-245

[6] Hong Qu, Jiuyuan Huo.2012.Design and Implementation of Digital Campus Project in University.Advanced Information Technology in Education, AISC 126:89~94

[7] Qian Wang, Nai Jia Liu, and Zhi Rui Cheng. 2012.The Application Research of Data Exchange Technology in Digital Campus. ISc IDE 2011, LNCS 7202, 607–613

[8] Xianmin Wei.2011.Research of College Information Integration and Sharing System. International Conference on Advances in Education and Management ISAEBD 2011.Part IV, CCIS 211: 615~619