Research and application of computer information system security technology in the new situation

Chenghai Cao

College of Industry Trade, Jiangxi Vocational Technical, Nanchang, Jiangxi, China

Keywords: New situation; Computer information system security; Safety technology; Teaching

Abstract: With the advent of the Internet era, computers have also entered thousands of thousands of families in their unique growth mode, and quickly become an essential part of their daily life. At the same time, some unlawfully unlawfully invaded the computers of enterprises, institutions and even individuals using the Internet, stolen the confidential data on their equipment or tampered their original data, which caused extremely bad political and economic losses to people's work and life. Therefore, the computer information system security technology has also aroused the attention of the people, and the major colleges and universities have also set up the computer information security technology courses in the computer major, and some universities have established the information security specialty. This paper mainly discusses the research and teaching application of computer information system security technology under the new situation.

1. Introduction

With the advent of the Internet era, computers have also entered thousands of thousands of people's homes in their unique growth mode, and quickly become an essential part of their daily life. According to the data, by the end of 2012, the broadband penetration rate in mainland China has exceeded 30%. At the same time, more and more enterprises and institutions have set up a set of business information management system which belong to their own, so the security problem of computer information system has gradually reflected people's vision. According to the survey statistics: only in 2012, the number of domestic first-class domain name sites tampered with 28,405, of which 314 educational sites were tampered with. And it's just the data that people find, and there are still a lot of hackers in a high level of concealment, so that people can't find out. According to a large enterprise manager, the internal network of the company had been hacked and controlled for several months when the administrator was unaware. Similarly, there have been similar events in the world: the most prominent global computer information development in the United States also has more than 10 famous Internet stations that have been attacked by black websites, resulting in a direct economic loss of up to $1 billion 200 million, and the most developed Japan in Asia, whose supreme court had suffered more than 3000 times in 3 days. Hacker attacks. Therefore, how to improve the security of computer information system has become a global strategic problem.

2. Main technology of computer information system security

The development and application of the computer information security technology and the computer information technology are mutually echoing. With the rapid development of the global political economy, the status of the computer information technology is increasing. Understanding and mastering the knowledge and technology of computer information security has become one of the basic skills of the young scholars in the generation. In terms of computer information system security technology, it can be simply divided into five categories:

2.1 Digital signature and authentication technology:

The so-called digital signature and authentication technology means that the creator encrypts the digital coded information with the public key of the recipient and sends it to the recipient with the original. The receiver can only use its own private key to unlock the encrypted digital encoding

  DOI: 10.25236/mmmce.2019.010

information, and then use the function HASH to generate a digital encoding information to the received information, and compare it with the decrypted digital encoding information. If the result is the same, it shows that the security of the transmission process is not tampered, the information is complete, and on the contrary, the information transmission has been modified, so the digital signature can verify the integrity of the digital encoding information. Therefore, the digital signature is the encryption process, while the digital signature authentication is the decryption process.

2.2 Firewall technology:

A firewall is a barrier that separates the public network from the internal network of the computer. In order to realize the security of the daily network, the potential aggressive invasion can be isolated as far as possible. In fact, it is a kind of isolation technology.

2.3 information encryption technology:

Information encryption technology mainly includes data transmission encryption and storage encryption two major aspects. When data transmission is encrypted, the main encrypted object is the data flow on the way of transmission, and there are three common ways: node encryption, end to end encryption and link encryption. The encryption system is divided into four parts: unencrypted message (plaintext); encrypted message (ciphertext); encryption and decryption equipment; encryption and decryption key.

2.4 Intrusion detection technology:

Intrusion detection mainly rely on IDS intrusion detection system to complete, its role is a reasonable supplement to the lack of firewall, the main help the system to deal with the attack from the network hackers, enhance the system security management ability, improve the integrity of the overall structure of information security. Intrusion detection can be roughly divided into two kinds of real-time intrusion detection and post intrusion detection.

2.5 Access control

Access control is the most critical technology in computer information system security. According to type, it can be divided into two categories: autonomous access control and mandatory access control. It refers to the privilege of limiting the user's access or use of some information items according to the user identity or the definition it belongs to. It is mainly applicable to the system administrator to control the user's access to the network, such as its servers, directories and files.

3. Current teaching situation of computer information system security course

The course of computer information system security is complicated and complicated. It is mainly to train students to understand the security settings, security vulnerabilities and security protocols in the current mainstream network system, to master the general security problems and defense strategies that may exist in the computer information system, and to improve the computer information system security of students in an all-round way. Full protection consciousness and safety protection ability. As far as the current study situation of universities and colleges is concerned, the situation of students' knowledge of curriculum is not ideal, and the expected results have not been achieved in the course of offering courses.

3.1 The curriculum involves a wide range of knowledge and fast updating of knowledge system.

The course of computer information system security involves numerous and complicated subjects, which mainly include information security technology, cryptography, network technology, computer science, communication technology, number theory, applied mathematics and information theory. It is a subject of OECD, which covers a wide range of contents. It needs not only the

knowledge of basic principles but also the skills of application and scheme design. In a word, the teaching content of the course includes the following aspects: information system security, information security overview, key distribution and management technology, cryptography foundation, network security, access control, security management, security audit, and so on. It is a comprehensive course in the university period. Therefore, there is a very high basic knowledge requirement for the students studying this course, but since the Ministry of Education issued the Ministry of education on the issue of the Ministry of education on the further strengthening of the subject of information security, the construction of professional construction and the training of talents in 2005, and the establishment of the “teaching and Guiding Committee of the higher school information safety class” in 2007, The major schools and computer related majors have set up information security classes and information security specialties. Schools have not targeted students of different types and different levels, and some schools should begin to develop early to students in the first three or four classes to make students learn. Difficulty and learning pressure have been greatly improved, and interest in learning has also decreased.

With the rapid development of the social economy, the computer technology and the Internet technology are changing with each passing day, as well as the methods of attack and prevention of hackers. There are many new network technologies, such as wireless sensor network technology, P2P network technology and so on, and many new network computing environments are also being born. As soon as students understand the knowledge of textbooks, new knowledge of computer information security has begun to appear in the society. Therefore, in the computer information system security teaching, it is necessary to keep up with the development trend of the information technology in the times, and still need to prepare new challenges to the information security technology at any time. 3.2 single teaching mode and contradiction between theoretical teaching and practical ability training.

As far as the content of the computer information system security course is concerned, the description of the vast majority of the principles is very Abstract, making this course extremely boring and difficult for students to understand. At present, the majority of school classroom teaching is still based on traditional teaching mode: pre-class preview teacher talk student questions. But in these three links, pre class preview is in a project that can not be effectively checked, and the students' questioning links are usually few students to ask questions, so the disadvantages of the traditional teaching model are obvious.

According to the investigation, it is found that the teaching content of the computer information system security course has a certain gap with the actual application of knowledge, which makes the course encountered a lot of confusion in the actual teaching process. Because the information system security technology is a new subject, and it has a close relationship with the real life and work study, many students have had a preliminary and shallow contact in their life before the beginning of the course, which encourages students to have great expectations when they have just touched the course. With the gradual progress of teaching progress, students quickly find that they can not effectively carry out the theoretical knowledge learned in the classroom with the practical application of life, so that students' interest in learning is gradually decreasing. As far as the practice course is concerned, there are still many practical links in the high school, which can not contain the content of the teaching theory, the reason is that the total number is too small. And according to a university teacher, many schools that have opened such courses still have no perfect information security laboratory and related experimental equipment, and many experimental projects can not be carried out. Therefore, how to cultivate and improve the students' experimental ability teaching has become an urgent problem to be solved urgently for the teaching of computer information system security course.

4. Teaching strategies of computer information system security course in the new situation

4.1 Distinguish between professional and practical selection of content teaching

With the rapid development of computer technology, colleges and universities have gradually

regarded the training of computer science and technology personnel as one of the most important tasks. According to the enrollment scale at this stage, computer information system security courses have been set up in all major undergraduate colleges and universities, and it will become a major. As far as the employment needs of students are concerned, colleges and universities, when students enter the junior study stage, will distribute them according to different professional direction to teaching. But the computer information system security course is still in sync, and some scholars have proposed whether the computer information system security courses can also be divided into different professional directions for special teaching. At present, the teaching materials of computer information system security course can be divided into two categories: theoretical teaching materials and practical teaching materials, because of the knowledge of cryptography in the theoretical textbooks and practical skills in practical teaching materials. The practical interest in the practical operation of the teaching materials is very large. Teachers can set up more experimental courses according to the students and introduce the importance of theoretical knowledge in the experimental course, and promote the common development of both students' theory and practice.

4.2 Improvements of teaching methods -- the combination and infiltration of traditional teaching and modern teaching

In the face of different teaching materials, teachers can also make teaching methods according to different teaching contents, and use the advantages of traditional teaching methods at the same time to quote new teaching methods, effectively combine traditional teaching with modern teaching, and get more outstanding teaching effect. Taking the theoretical course as an example, because some of the theoretical knowledge in the computer information system security course is more Abstract and complicated and difficult to understand, the teacher needs to change a single traditional teaching mode. It can use the interesting teaching method in the modern teaching way to drive the students' interest in learning to be active and improve the students' active learning ability. In this way, the effect of teaching can be doubled. In the course of teaching practice, the traditional teaching mode should be used more, so that the students can make the experiment more obvious after understanding the content of the study in advance.

References

[1] Fan Ying, Fan Yonghai: An Analysis of the Present Situation and Development Prospects of Computer Information Security Technology, Dalian Maritime University Press [J], 2009 (05)

[2] Ren Li Feng: Research on computer information security technology, development of high technology [J], 2011 (01)

[3] Sun Xiaoyan: Discussion on Teaching of information security technology, value engineering [J], 2011 (02)

[4] Dai Guoyong: teaching practice and thinking of computer information security course, Journal of Zhejiang Shuren University [J], 2011 (04)

[5] Li Hongjiao, Wei Weimin, Yuan Zhongxiong: Thinking on the teaching of the course of information security for computer science and technology, 2011 National Symposium on cryptography and information security, [J], 2011 (01)