The Application Research of Computer Security Technology in E-commerce

Mei Zhao[1, a]

[1]Shandong Institute of Commerce and Technology, Jinan, Shandong, China

[a]e-mail: 20811276@qq.com

Abstract. Aiming at many security problems existing in the current e-commerce transaction process, this paper will build an e-commerce security alarm system based on computer security technology, which integrates two application cores, virus detection and security prevention, under the Web application service architecture system. In the aspect of virus detection, the system will adopt Signature scanning model, Checksum calculation model and Software simulation to deal with the intrusion of various computer viruses into e-commerce system. As for security prevention, the system comprehensively uses Firewall, Digital signatures and Digital encryption to effectively avoid the harm caused by stealing private information, counterfeiting transaction information and malicious destruction of content. The system will help to improve the security of e-commerce trading environment and create better convenience for people's life.

Keywords: E-commerce; Computer security technology; Feature code recognition technology

1 Introduction

The E-commerce refers to a certain kind of online trading activities that take electronic technology as the carrier of development and business as the core. As compared with the traditional offline entity sales, the online sales channel provided by e-commerce has broken the geographical limitation of the traditional economic transaction process, and at the same time, it has reduced the development cost by more than 30%. At present, it has become an important part of people's life. At the same time, the development of e-commerce is also faced with many security problems, such as computer viruses, information leakage, etc. How to give full play to computer security technology to create a good e-commerce operating environment is also the research focus in the current development process.

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 219–226, 2022.
https://doi.org/10.2991/978-94-6463-108-1_25

2 Application of computer security technology in E-commerce

2.1 Virus detection technology

1) Characteristic code identification technology.

When detecting viruses, the commonly used detection technology is the characteristic code identification technology (as shown in Figure 1). Its main function principle is to record the characteristic codes of viruses and store them in the virus resource database. When faced with the antivirus demand, you can compare the scanned contents with the information in the database. After the similarity exceeds the safe value of 80%, you will determine that the computer has been infected with viruses, and you will deal with them accordingly, so as to play the role of computer antivirus. This method has a simple operation process in practical application, and the detection rate can reach more than 90%. It has been applied in many computer virus killing. However, this method also has some limitations, only known viruses can be detected, and unknown viruses will default to safe files. For this reason, it is necessary to update the database irregularly to meet the needs of computer virus killing.

There are many types of common feature code algorithms. This system will focus on MD5 algorithm as the feature code. MD5 generally refers to the hash transformation of byte strings, that is, converting byte strings of any length into an integer of 128bit. In the process of judging virus files, MD5 algorithm is irreversible, and has obvious efficiency and stability. As shown in Figure 2, it is the key code to realize the virus detection function of MD5 signature.

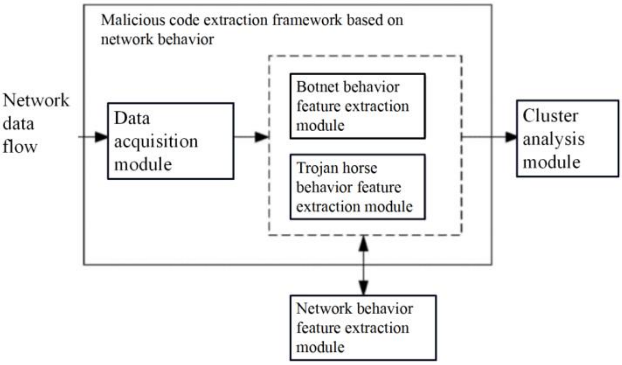
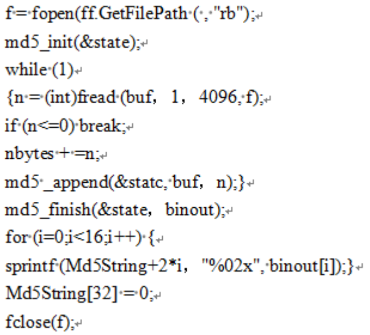

Malicious code extraction framework based on network behavior
Network data flow
Data acquisition module
Botnet behavior feature extraction module
Trojan horse behavior feature extraction module
Cluster analysis module
Network behavior feature extraction module

Fig. 1. Schematic diagram of application process of characteristic code identification technology



```
f = fopen(ff.GetFilePath ( , "rb");
md5_init(&state);
while (1)
{n = (int)fread (buf， 1， 4096, f);
if (n<=0) break;
nbytes + =n;
md5 _append(&statc, buf， n);}
md5_finish(&state， binout);
for (i=0;i<16;i++) {
sprintf (Md5String+2*i， "%02x", binout[i]);}
Md5String[32] = 0;
fclose(f);
```

Fig. 2. Code for realizing virus killing function of MD5 special detection code in C++

2) Document verification and identification technology.

By summing up the experience of computer virus killing in the past, we can know that when computer viruses invade computers, they don't exist as separate files, but are usually registered in a certain program. If the file takes up more space and the date of the file changes, the surface system will be infected by a virus. The main principle of file verification and identification technology (as shown in Figure 3) in application is to check the files in the hard disk once while ensuring the safe operation of the computer, and record the relevant information of the files (such as occupying space and changing time, etc.). In the subsequent virus killing, it will be mcrc again. If the qualified rate of parameters is lower than 60%, then the virus infection of the files can be considered, and then targeted treatment can be carried out. This method can identify known and unknown viruses, and it is a technology type that is widely used during the current e-commerce operation.

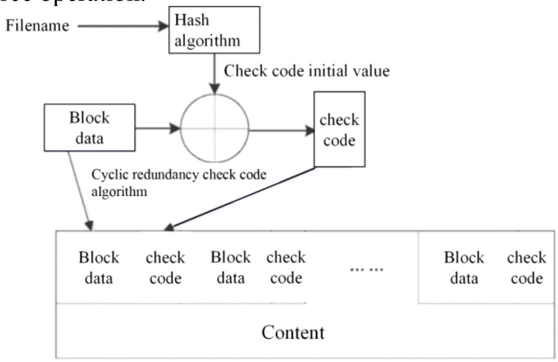


Fig. 3. Schematic diagram of document verification and identification technology

3) Software simulation technology.

During the application process of this technology, its technical application principle lies in copying the current working state of the computer, then simulating the running state of the structure, comparing the current running state with the conventional running state, finding out the differences among them, and further identifying them, so as to discover computer viruses and improve the rationality of the running mechanism. Although this method can simulate the computer operation, its efficiency is relatively low, only 70%-80%, according to the application of e-commerce. However, for some encrypted viruses that can't be located and identified, this technology can be used to make accurate judgments, so as to quickly eliminate stubborn viruses.

4) Pre-scanning identification technology.

The computer virus identification technology is a method of copying and identifying the running state of the computer on the basis of simulation. In the specific application, the pre-scan recognition technology mainly starts from simulating the running state of CPU, and its simulation content goes deep into the basic structure of computer. In theory, this technology can accurately identify any form of computer viruses during the operation of e-commerce, and can thoroughly eliminate some intractable viruses. But the independence of the technology is relatively poor, so it is necessary to use other intervention technologies for pretreatment before use, so as to avoid the spread of the virus, which is the main reason for the slow popularization of this technology at present.

2.2 Safety prevention technology

1) Firewall technology.

The technology has been applied for a long time, which is a method to isolate the dangerous content encountered during the computer operation from the "wall", and it is also an important reliance to ensure the safe operation of the computer. This technology has the functions of network filtering and information isolation in specific applications, and can actively deal with the intrusion of computer viruses. And in the process of firewall technology application, we can also trace the corresponding data sources in and out of the computer according to the user's defense strategy, so as to shield the illegal computer window from the root, and at the same time, we can reasonably control the network connection and isolate 100% dangerous viruses from the e-commerce network, so as to ensure the safety of information used in safe areas. For example, in Taobao's "Double Eleven" Carnival in 2019, the total number of transactions in a single day exceeded 100 billion yuan, which also included many online transaction records, which also needed to be protected by firewall technology. At the same time, it also needed to optimize the technical applicability and functionality, thus playing a role in optimizing the computer running environment [1].

2) Intrusion detection technology.

In the application process, this technology mainly detects the reserved information after malicious attacks and intrusions, so as to identify viruses. As shown in Figure 4, during the application period, the technology itself has certain analysis and processing capabilities. Based on the integration of computer logs, Internet access records and other contents, it can identify the current working state of the computer, which is also the content that the detection system needs to focus on during the application period.

Therefore, the key content of this technology in the application process is the data information processing effect. In order to improve the practicability of the data processing effect, statistics, expert system, neural network and other technologies will be used to process the e-commerce transaction data in the specific processing process, so that during the application period, the Internet anti-virus system can make a positive response and effective defense to the invading virus in ns level, and then improve the security of e-commerce operation [2].

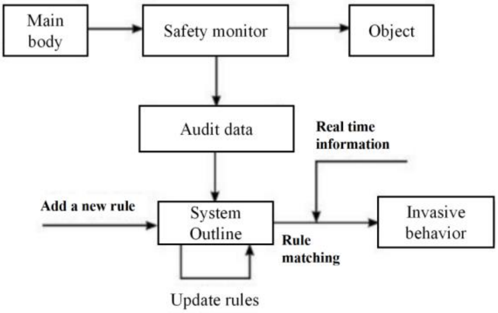


Fig. 4. Application model of intrusion detection technology

3) Safety evaluation technology.

During the application of this technology, its main preventive principle is to monitor the stored state data. In application, when there is data flow in the computer, it will collect the generated real-time data. After the integration of e-commerce operation data, it will compare this data with the standard data stored in the database. According to the data comparison result (80% for example), it will evaluate whether there is any abnormality during the computer operation. At the same time, in the process of technology application, the application of security hardware, software and security protocols in the computer system will be supervised to evaluate whether the system behavior is reasonable. During the application process, the security evaluation technology not only aims at the behavior of computer viruses, but also needs to supervise the situation of the computer running itself, and it also has a great chance of being attacked by computer viruses in application. Therefore, it is also necessary to update the system software and hardware in practical application, so as to improve the reliability of e-commerce running.

4) Digital signature technology.

The digital signature technology is to add some data content to the data unit or change the password of the data unit. This technology can not only determine the source of the data unit, but also ensure the integrity of the data unit, thus achieving the goal of protecting the data. The most important thing is to prevent the data from being forged by the transferee. In addition, digital signature technology is also a way to sign messages in electronic form, and a signature can be transmitted in a network. The digital signature technology can encrypt the abstract information, and then send the original text to the receiver together, and the receiver can decrypt it only by using the public key. Then, the HAVH function is used to generate a summary information of the received original text of e-commerce, and then it is compared with the decrypted summary information. If the comparison is the same, it means that the information received by the receiver is complete; otherwise, it means that the information content has been maliciously tampered with [3].

5) Data encryption technology.

In order to effectively improve the security of e-commerce activities, more efficient technologies are needed, and data encryption technology has certain advantages, which can guarantee the security and stability of e-commerce transactions. The data encryption technology is to encrypt the plaintext, so that the plaintext will be converted into ciphertext, and the receiver only needs the decryption algorithm to convert the ciphertext into plaintext (as shown in Figure 5). As far as encryption algorithms are concerned, they are mainly divided into private key and public key. The former is also called symmetric key, that is, the same key is used to encrypt and decrypt files. This algorithm has the advantages of simplicity, ease and wide application. The latter is encryption and decryption by using no key, which has the advantage of higher security. However, because two keys are needed, the latter algorithm is relatively difficult and it is difficult to identify the sender.

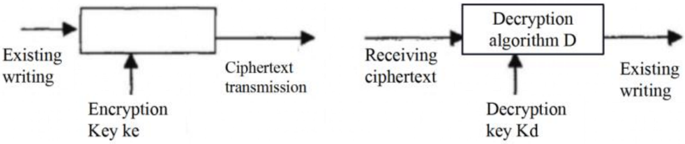


Fig. 5. Schematic diagram of data encryption technology

2.3 Proposed alarm system

1) Analysis of monitoring mechanism.

In the working process of the virus alarm system, its monitoring mechanism lies in using the system to understand the basic situation of the virus, which also needs to be completed by using computer probes, whose positions are generally set at the entrance of the subnet. At this time, the reported data information is collected by using the particularity of the virus itself. During the data integration analysis, the main processing technology used is characteristic code identification technology, which is used to determine whether the system has been infected with computer virus. Especially when faced with unknown viruses, the system can be used to identify the parameter information, so as to truly restore the actual application situation, which also greatly accelerates the virus detection efficiency and improves the virus prevention effect [4].

2) Overall structural design.

In the overall design of the early warning and detection system, a multi-line design will be adopted, and at the same time, the virus alarm system will be optimized with the method of centralized layout. In the specific design process, it is necessary to design the monitoring probe at the network interface position, which is used to monitor the operation of the computer, collect the working information of the computer and transmit it to the processing mechanism for centralized processing, so as to reduce the controllability of the system. And the management center will also concentrate on processing the monitoring data. While clearing the running virus to the outside world, it can also study some complex cases, and make clear the transmission routes and conditions of the virus, so as to improve the stability and timeliness of computer alarm performance [5].

3) Subnet Division Model Expansion.

During the traditional subnetting process, its model is mainly shared, and in application, many computer groups will participate in the interaction, so as to improve the accuracy of data collection. With the rapid development of Internet technology, the richness of network development mode is also increasing. Based on this, it is necessary to improve the detection requirements appropriately, so that it can meet the application effect of the current switched network. Moreover, in the process of system application, it is also necessary to fully recognize the advantages of subnet model in application, and sort out the application points of relevant subnet models, so as to reduce the probe pressure and improve the final application effect of the model [6].

4) Expansion of detection model.

At present, with the continuous improvement of the maturity of network technology, the CPU processing capacity of computer system has been greatly improved. In order to meet the functional requirements of the system, it is also necessary to adjust the application of network bandwidth, so that it can meet the working requirements of probes and broaden the defense system of computer viruses. In the application of probe system, it is mainly composed of shunt and data processing mechanism. And the system will use a node machine to process data within 400M, while over 400M will complete the data classification processing according to the excess situation, so as to improve the compliance and practicality of e-commerce operation [7].

3 Conclusions

In conclusion, from the current development situation, e-commerce has created a lot of convenience for people's lives. At the same time, the problems about the safe operation of e-commerce are also highlighted. How to improve the ability of e-commerce security prevention has also become the focus of research. In the research process of this paper, some prevention experiences and technical ideas in other fields have been studied, and based on this, the current computer security application system has been improved, which has positive guiding significance for the in-depth research of computer security technology.

References

1. Xiong Ning (2021). The Application Analysis of Computer Security Technology in E-commerce. Network security technology and application.(04):99-100.
2. Yun Pengyu (2021). The Application of Computer Technology in E-commerce from the View of Security. Digital Space.(04):53-54.
3. He Chunhua (2020). The Application of Computer Network Security Technology in E-commerce. Digital Space,(12):255-256.
4. Zhang Yanting (2020). The Application Analysis of Computer Security Technology in E-commerce. China New Telecommunications.22(22):134-135.
5. Wang Gang, Yang Ning, Yu Xiaona (2020). The Application of Computer Security Technology in E-commerce Transactions .China Computer&Communication.32(19):12-15.
6. Zhang Yumin (2020). The Application of Computer Network Security Technology in E-commerce .China Computer&Communication.32(15):198-200.
7. Han Shufang (2020). The Application of Computer Network Security Technology in E-commerce. Electronic technology and software engineering.(15):231-232.