Computer Network Security Processing Based on Big Data Environment

Fan Gaozhi

College of Engineering and Technology, Hainan College of Economics and Business, Haikou, Hainan, 571127, China

Keywords: Big data; computer; network security processing

Abstract: In the process of continuous development of modern society, it is necessary to meet the needs of the times and strengthen the construction of technical security. Computer network technology has been used in various industries and has a certain impact on the normal operation and development of social production and life. This paper focuses on the analysis of computer network security processing technology in the context of big data.

1. Introduction

In the process of accelerating the development of modern social economy, the network information platform has become an important carrier for people to communicate. In the context of the era of big data, computer network security is particularly important, and it has a direct impact on the safety of the public and property. However, some of the lawlessness has extended the devil's talons to the network information platform. Hackers have seriously threatened the security of network information in the context of the era of big data. Great importance should be attached to the security of big data computer networks in this regard. The external environment of information security is cleared based on the level of information security of computer network, so as to improve the efficiency of countermeasures and control the computer network information security, Thereby promoting the stable and safe development of society and economy.

2. Computer network security issues in big data environment

2.1. Hacking

The popularity and use of the Internet has brought convenience to people's work and life. However, computer hackers and the illegal behaviors have also appeared in this process to make an impact on the continuity and stability of computer information data, and even lead to paralysis of the system, which seriously threatens the security of computer network information. Hackers attack mainly includes two aspects, the first is active attack, the second is passive attack. And the active attack behavior refers to the hacker's destruction and attack on some data information in the computer network information system, which leads to the omission and loss of computer data and information, thus bringing certain losses and troubles to people's work and life. In addition, hacker's passive attack can intercept information and data by passive cracker, resulting in different degrees of harmful consequences.

2.2. Natural disaster

Because the external equipment of the computer is fixed, the machine itself can not effectively resist the destruction of the external environment, which leads to the computer can not guarantee the safety of the machine components in the face of computer disasters and pollution, vibration, water and fire threats and thunderbolt caused by accidents. Therefore, the vulnerability of the machine itself also has an impact on computer network security factors.

2.3. The openness of network

Computer network has the characteristics of openness based on its wide application, which also leads to the vulnerability of computer network system itself. Because of the openness of network,

  DOI: 10.25236/csam.2019.047

the security of Internet using TCP/IP protocol is relatively low, which leads to the lack of security of the network itself. And the data function and service function can not meet the demand in the process of running the protocol with low security. Therefore, the openness of the network itself will also affect the security of the computer network.

2.4. Computer virus

In the era of big data, computer networks have obvious openness, which makes the concealment of computer virus intrusion more prominent. Computer viruses are characterized by execution, concealment, and storage. When the virus is loaded into the program, he latency, infectiousness, triggerability and destructiveness of the virus itself is manifested, which seriously jeopardizes the network data. The main subject of network virus transmission is that the virus runs in the program in the process of data flow. It will lead to a greater threat for viruses with strong harmfulness.

2.5. Operational errors of people

At present, the public work and life have a close relationship with computers. Most people get information, storage information and transmission information through their computers every day. Only when computer users make scientific and correct operations can the computer functions be fully utilized, so as to facilitate users. However, if the user's personal operation fails, it will bring hidden dangers to the computer system, which is very harmful to the protection of network information security. Computer users of different levels have different computer network protection awareness and operational capabilities. Users may encounter hidden dangers of computer network because of their computer misoperation in their daily lives.

3. Computer network security processing strategies in big data environment

3.1. Using firewall technology

In the context of modern big data, computer users can interfere with the operation of computer-based malicious software through firewall technology, thus improving the security of computer network information. The firewall technology is divided into three types according to the technical characteristics: conversion, packet filtering and proxy. The use of different firewall technologies enables computer users to create a safe and healthy network environment, preventing the lawbreakers from stealing information by illegal means. Although the firewall can block non-access data and information, it can not block the virus. Then, it is necessary to be reasonable in the process of using the firewall to protect the network information transmission and reception. Figure 1 shows the settings of the firewall technology.

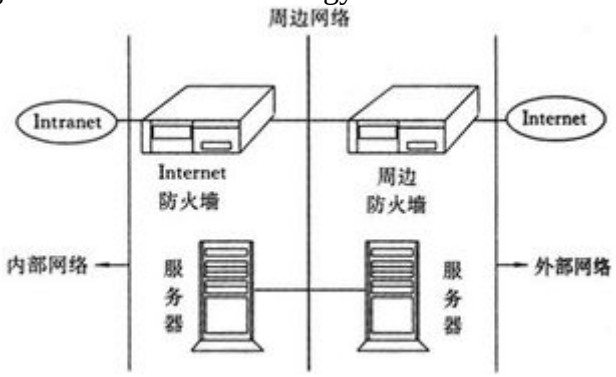

Figure 1 Firewall technology settings

Check port and firewall status: #netstat -lnt |grep 80
Enable 80 port command: /sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT
Save the configuration command: /etc/rc.d/init.d/iptables save
Restart service command: /etc/rc.d/init.d/iptables restart
Check the open ports: /etc/init.d/iptables status

3.2. Perfection of network monitoring management system

It is necessary to consider the social individual, administration and legislation in terms of the macro-strategy. The national legislature should promote the legislation of the individual and subject liability of network information security impairing, so that the corresponding case handling can not just stay at the level of administrative punishment and can not form an effective deterrence. The administrative department shall perfect the corresponding system and implement it strictly in accordance with the standards, and complete the work through network security monitoring and management to effectively realize computer information security. The responsibility consciousness of the network operation platform and the corresponding software developers should be improved. Internet enterprises should have social consciousness to take the initiative to cooperate with the implementation of national Internet regulatory measures, and safeguard the network security rights and interests of the broad masses of the people through appropriate means.

3.3. Raise hacker's attack consciousness

In the era of modern big data, people are not surprise about hacking attacks and stealing information, but they can not be neglected to guard against it. Firstly, relevant enterprises realize the establishment of a trusted hacker attack prevention management system, thereby realizing the identification of hackers stealing behaviors. And they effectively use firewall technology to optimize the performance of network information security, so as to reduce the possibility of hacker attacks. In addition, the corresponding enterprises also need to effectively promote the use of computer network data authentication technology, so that the distribution channels of computer network data authentication technology can be expanded and the safe operation of computer network can be effectively controlled.

3.4. Network monitoring technology

Network monitoring technology can also monitor LAN computing, including monitoring of online behavior, and it can also improve the efficiency of data information security management. Internet monitoring software can manage online behaviors, audit network behaviors, and check the information and data content, such as web browsing, email, chat and traffic. The intranet monitoring software can manage intranet behaviors and computer screens, as well as monitor the security of computer hardware and software information data and equipment assets, including print monitoring, screen monitoring video recording and application software restrictions. Figure 2 shows the network monitoring setup structure.

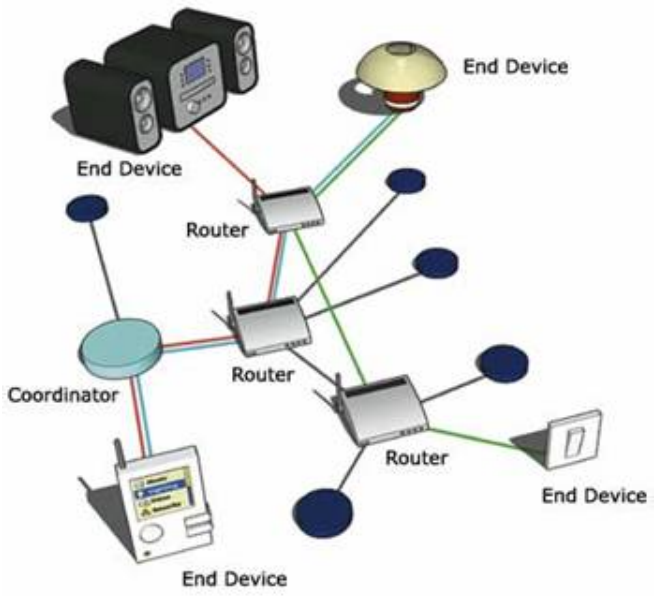

Figure 2 Network monitoring setup structure

3.5. Encryption technique

The use of encryption techniques in e-commerce can effectively protect it and encrypt data information through the technique. This paper uses DES encryption algorithm, which can also be called data encryption standard. The DES algorithm has three entry parameters, namely Key, Data, and Node. And the Key is seven bytes, a total of 56 bits, which is the working key of the DES algorithm. Data is eight bytes and 64 bits, which implements encryption and decryption of data. Mode is the mode of operation of DES, including encryption and decryption. The following is the main code for the encryption technique:

```
* Encryption
* @param datasource byte[]
* @param password String
* @return byte[]
*/
public static    byte[] encrypt(byte[] datasource, String password) {
try{
SecureRandom random = new SecureRandom();
DESKeySpec desKey = new DESKeySpec(password.getBytes());
//Create a key factory and use it to convert the DESKeySpec
SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES");
SecretKey securekey = keyFactory.generateSecret(desKey);
//The Cipher object actually completes the encryption operation.
Cipher cipher = Cipher.getInstance("DES");
//Initialize the Cipher object with the key
cipher.init(Cipher.ENCRYPT_MODE, securekey, random);
//Now, get the data and encrypt it
//Formally perform encryption operations
return cipher.doFinal(datasource);
}catch(Throwable e){
e.printStackTrace();
}
return null;
}
/**
* Decryption
* @param src byte[]
* @param password String
* @return byte[]
* @throws Exception
*/
public static byte[] decrypt(byte[] src, String password) throws Exception {
// The DES algorithm requires a trusted random data source
SecureRandom random = new SecureRandom();
// Create a DESKeySpec object
DESKeySpec desKey = new DESKeySpec(password.getBytes());
// Create a key factory
SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES");
// Convert the DESKeySpec object to a SecretKey object
SecretKey securekey = keyFactory.generateSecret(desKey);
// The Cipher object actually completes the decryption operation.
Cipher cipher = Cipher.getInstance("DES");
// Initialize the Cipher object with the key
cipher.init(Cipher.DECRYPT_MODE, securekey, random);
```

```
// Actually start the decryption operation
return cipher.doFinal(src);
}
}
```

4. Conclusion

At present, the requirements for computer network information security are relatively high. Then, it is necessary to attach importance to the protection of computer network information security and to create a complete and scientific network information protection system, so as to improve the level of network information security protection, thus maintaining the interests of network users.

References

[1] Jing Zhang, Bo Qin. Computer Network Security Prevention in the Background of Big Data [J].Chinese Information, 2018,(11):7.

[2] Zhao Li. Analysis on Computer Network Information Security in the Big Data Era [J].Chinese Information, 2018, (11):3.

[3] Yu Qi. Research on Computer Network Information Security in the Age of Big Data [J].Sciences & Wealth, 2018, (31):27.

[4] Xiangbo Liu. Computer Network Information Security and Protection Measures in the Background of Big Data [J].Shu ZiHua Yong Hu, 2018, 24(44):151.