Retraction

Retraction: Analysis of Network Intrusion Detection Technology Based on Computer Information Security Technology (J. Phys.: Conf. Ser. 1744 042038)

Published 16 September 2022

This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity. In addition, IOP Publishing has seen no evidence that reliable peer review was conducted on this article, despite the clear standards expected of and communicated to conference organisers.

The authors of the article have been given opportunity to present evidence that they were the original and genuine creators of the work, however at the time of publication of this notice, IOP Publishing has not received any response. IOP Publishing has analysed the article and agrees there are enough indicators to cause serious doubts over the legitimacy of the work and agree this article should be retracted. The authors are encouraged to contact IOP Publishing Limited if they have any comments on this retraction. Retraction published: 16 September 2022
Analysis of Network Intrusion Detection Technology Based on Computer Information Security Technology

Xinzhou He¹,*
¹Changjiang Polytechnic, Wuhan, Hubei, China, 430074
*Corresponding author e-mail: 343221@cjxy.edu.cn

Abstract. Data is the basis of information technology security management, with the arrival of the era of big data, computer network security is also facing a lot of challenges, we all know that the network has many characteristics: open, virtual characteristics, which there are a lot of security risks. So we must strengthen the network security analysis, explore the main network security hidden danger, and put forward the corresponding to the computer information network security precautions, now is the information age, big data is the basic characteristic, and the Internet technology widespread application, computer network security problems often appear, often have all kinds of viruses into our computer, so we also want to strengthen the network security management, and puts forward the countermeasures, so as to improve the level of safety in network, strengthen network security protection, it is very important[1].

Keywords: Big Date, Computer Network, Security

1. Computer network security in the era of big data

1.1. Lack of understanding of network security

In the context of big data, people can use the Internet to enrich their lives and simplify their work. But everything has a good side and a bad side, and with that comes the risk of network security, information leakage, user security and other issues. Because most of the management of network security staff lack of awareness to maintain network security, resulting in computer security problems and the emergence of information leakage incidents. First of all, many people who use the Internet have no faith in themselvesI have enough knowledge about security, and I haven't installed some intercepting software in the process of using it, so I haven't done the protection work, which leads to a lot of loopholes in information security[2]. Secondly, network management staff in the prevention of network vulnerabilities attitude more perfunctory, there is a fluke psychology, network security prevention and information disclosure did not pay attention to, and step by step to expand the computer network security vulnerabilities. Finally, groups, schools, enterprises and other organizations generally have LAN, if the security management personnel do not properly protect, more do not have the awareness of security risks, then once the information in the network is leaked, it will bring a lot of economic losses to the organization.
1.2. Illegal ACTS on the Internet
There are many learning, entertainment and life software in the Internet, and it is hard for people to avoid these software and websites when using the Internet. There are loopholes in most websites, and even some of the people who designed the original websites put some backdoor data in the background for their own personal use, but if hackers in the network take advantage of it, then the website operators and users will suffer great losses. In addition, the virus in the network - like can become a network attacker, although people's computer antivirus software has been protecting the computer, but there are policies, countermeasures, the network virus is still in a variety of ways to break into people[3].

![Figure 1. Computer information.](image)

In computers to get information about people. Some even use Internet viruses to obtain other people's information and pictures for blackmail threats. The form of vulnerability and hidden trouble in the computer is changeable, people may be used at the same time inadvertently be invaded, thus revealing personal privacy, leading to computer failure.

There are massive amounts of information every day, including network log, video, audio and text, etc. These information resources have a large base, but there are few useful information. Therefore, traditional data mining technology cannot improve the validity of information processing more effectively. All kinds of network information and resources under the background of computer network: sharing, strong openness. The huge virtual space for criminals to provide the possibility of network intrusion to computer network security threats. - It is hacker intrusion, which is an important security threat of network intrusion in the era of big data. - Some hackers take advantage of computer network vulnerabilities to invade the computer system of others, steal network information, data to do some damage to the behavior or others to bring a direct impact on computer network security. The other is computer viruses. The so-called computer virus, is mainly to invade the computer network platform of all kinds of illegal programs, such as Trojan virus, spyware virus, script virus, etc. These network viruses spread fast, destroy other people's computer systems, launch vulnerability attacks, and manipulate the operating system to steal user information[4]. The network virus itself has strong concealment and high infection rate, which is harmful to network security. Users may encounter virus invasion without knowing it, which may bring system paralysis. Other information may also be stolen, tampering risks. Third, network system vulnerability. The vulnerability of the computer network system itself is mainly related to the program error and Bug of the software system. Usually, network system vulnerabilities have the potential, these security vulnerabilities once exploited by hackers, often cause huge property losses. For example, some hackers usually take advantage of the system's own security vulnerabilities to complete the invasion operation. And destroy or steal system resources. Fourth, insufficient awareness of network security management. In network management, the security awareness of operators is crucial. If the lack of security awareness, the network security risks caused by their own operational mistakes may bring threats to the network system operation and lead to virus invasion[5].

2. Computer network security analysis technology
For example, for the storage of log information, traffic data and other information, GBase and HBase
columns can be used to complete data retrieval and response in a short time, and Hahoop distributed management can be implemented according to the network security organization architecture, and analysis reports can be formed for Hive script mining. This method can automatically realize the security statistics and warning analysis of the data information of each node and store it safely by streaming mode. Second, data acquisition technology. Data collection is an important condition to ensure data integrity. Software such as Flume, Kafka and Storm are often used for data collection to realize effective integration and distributed management of data from different sources. However, in the data acquisition technology, the processing of streaming data should be carried out in Kafka cache format and the subsequent analysis should be carried out on the basis of row processing. Second, data retrieval should be carried out on the basis of big data retrieval in major counties, and the proportion of each section should be checked on the basis of ManReduce. The whole store. Second, data acquisition technology. Data collection is an important condition to ensure data integrity. Software such as Flume, Kafka and Storm are often used for data collection to realize effective integration and distributed management of data from different sources. However, in the data acquisition technology, The third is the retrieval of data. Data retrieval mainly USES big data and MapReduce as the retrieval basis to process the data of each node, and USES distributed parallel computing to complete data retrieval to improve the management efficiency of network anomalies. For example, the traceability method is used to find the hidden security data, and to locate, analyze and deal with it. Fourth, data analysis. Data analysis is to capture and monitor abnormal behaviors related to network security through complex event processing technology and customized wire connection analysis and calculation method. In non-real-time data analysis. On the basis of Hadoop architecture, with the help of data aggregation, situation analysis, offline statistical risk, data mining, data extraction and other technologies, to achieve the identification of network attack sources. Fifth, association analysis of multi-source data. In the context of big data, network security threats are diversified. How to improve the efficiency of network security analysis usually requires the collection and analysis of heterogeneous multi-source data within a specified time and the disposal of potential hidden sources. For example, the botnet can be analyzed by combining the characteristics of flow and DNS access, the query path of data source can be expanded, and the analysis of traceability data can be optimized to find and locate the traces or vulnerabilities that may be attacked, so as to make security prevention and treatment as soon as possible.

3. Computer network security countermeasures in the era of big data

3.1. Enhance the understanding of network security

In the era of big data, improving people's understanding of computer network security is one of the important factors to ensure information is not leaked. People should replace the name and password of their computer with complex letters, symbols and Numbers to increase the difficulty of criminals to invade, so as to improve the security of computer information. Because many users are afraid of forgetting their passwords, they will set up the same account and password on all websites and platforms. Therefore, websites and platforms need to pay attention to the password prompts when users register to avoid information security problems. At the same time, Internet users should also set up complex passwords on their WIFI to prevent intruders from stealing information through WIFI. Also, try not to use public WIFI to avoid information leakage. Network management personnel also need to improve their own awareness of prevention, for ensuring the occurrence of various safety accidents, enterprises and institutions should increase the professional level of security management personnel and professional ethics, and let the application of network workers and security management personnel to cooperate with each other, thus maintaining the internal information security of enterprises and organizations.
3.2. Resisting illegal network intrusions
Using network virus is a kind of non-material means, by attacking other people's computer network to steal information and obtain their own interests, network virus can have a direct impact on others' computer security. Therefore, users need to update their computer anti-virus software in a timely manner, and this extension, the construction of anti-virus security range, in case the network virus can pose a threat to the computer and network information. First of all, users can use anti-virus software and anti-theft system in the computer, and always check whether the computer has been illegally invaded, if the software prompts the existence of security holes in the computer, users need to timely repair. Users should be on guard at the same time when installing each software, open it after confirming it is green software, and dispose garbage regularly in the recycle station, to guard against virus breeding. Secondly, strengthen security prevention and computer early warning mechanism in the platform where data are stored to reduce the chance of virus invasion and protect the security of user information. Unknown urls sent by strangers cannot be opened at will, which is very likely to cause virus invasion. Finally, network information is also protected by law. Once users encounter criminals who steal information, steal property and spread their own privacy information, they can protect their own interests through network police and public security, and effectively protect personal privacy and property security. Cyber crimes should also be punished accordingly.

4. Conclusion
To sum up, in the era of big data, computer and network technologies have been widely applied in China, bringing people a very convenient application experience in life, work and entertainment. However, in the era of big data, there is connectivity and interactivity, which gives many criminals an opportunity to take advantage of. In addition, Chinese enterprises and institutions are also facing the threat of hackers and network viruses to information security. Therefore, enhancing the understanding of network security and resisting illegal network intrusion have become the necessary means to maintain information security at present. It is an important work under the environment of big data. We should actively introduce software and hardware technologies to prevent all kinds of network intrusion, hacker access and illegal operation. Improve the level of network security monitoring for computer network security to build a good operating environment.

Reference
[1] Xie Xiaomin, Establishment of Computer Network Information Security Protection Mode and Technical Analysis [J] Science and Technology Innovation, 2019(7) 66-67.
[2] Long Zhenhua. Computer network information security and protection strategies in the era of big data [J]. China management informatization, 2019, 22(6): 161-162.
[3] Baijie. Research on Computer Network Information Security and Protection Strategy in the Era of Big Data [J]. China New Communications, 2012, 20(15): 185.

[4] Zhao Siqi. Application of Computer Network Security Technology in Network Security Maintenance [J]. Satellite television and Broadband Multimedia. 2019(21): 37-38.

[5] Li Guoqiang. Reflections on the Application of computer network security Technology in network security Maintenance [J].

[6] Tan Mingbin: Application of Computer Network Security Technology in Network Security Maintenance [J] Computer Products and Circulation. 2019(9): 11.

[7] Yang Ge. The Importance of Enterprise Computer Network Information Security Management [J]. Abstract: Engineering Technology, 2016(3): 288.

[8] Wang Yuanxin, Wang Benyu: Research on Computer Network Information Security and Protection Strategy [J]- Reading Digest 2017.12(1): 00175.

[9] He Binying. Application of Big Data Technology in Computer Network Information Security problems - Comment on Computer Network Information Security [J]. Electroplating and Finishing, 2020(3): 47.