Retraction

Retraction: Development and Design of Network Security System Software Based on Big Data Analysis Technology (J. Phys.: Conf. Ser. 1992 022145)

Published 9 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This article has been retracted by IOP Publishing following an allegation that raises concerns this article may have been created, manipulated, and/or sold by a commercial entity.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: 9 September 2022
Development and Design of Network Security System Software Based on Big Data Analysis Technology

Xiang Wang¹, Zheng Li¹, Haiming Hong¹, Minghui Zhou¹,∗
¹China Gridcom Co., Ltd Research and Development Center, Shenzhen, China, 518000
*Corresponding author e-mail: zhouminhui@rdc.grid.org

Abstract. As an important part of the Internet field, big data has a wide range of applications in many fields. At present, neither study nor life can leave the network big data. But at the same time, issues related to network security have also attracted widespread attention from the public and professionals. Based on the knowledge of big data and computer network security, this article analyzes the threats to computer network security in the data age and discusses the development and design of relevant network security software.

Keywords: Big Data, Cyber Security, Software

1. Basic introduction between cyber security and big data

1.1. Concept of cyber security
Network security refers to the protection of information on the network from the impact of data leakage, modification, or destruction due to illegal use. It is indispensable to ensure the confidentiality and security of the information itself in many application fields such as computer, mathematics and communication applications. We also need to ensure that only authorized users have the right to process information as well as ensure that complete and accurate information can be provided in the process of processing and protecting information. Only in this way, when authorized personnel need to obtain information, they can obtain information resources without hindrance.

Network security includes several aspects: First, the security of cyberspace includes the maintenance of Internet infrastructure and other facilities; to ensure the normal operation of the network. Special attention should be paid to technologies such as Trojan horse destruction. Additionally, the destruction of hardware, Internet passwords and decryption should be noticed as well as bad content, misbehaviour, dangerous network content as well as the explosion of its own security issues during network transmission and so on [1].

1.2. The characteristics of network information security risks in the context of big data
In the context of big data, information security on the Internet has a series of characteristics:

(1) Concealment.
Virtual characters, individuals, and role participants have potential and hidden characteristics. The illegal acquisition of network information is not limited by space and time. Therefore, offenders may
be free in time and space, using black technology to steal network information. But due to the criminal process, there may be no traces and it is strenuous to be found.

(2) Intelligence.

In a broader scope, the information security risks in the network are very intelligent, which is because computer network professionals with extensive experience in this field will take advantage of network gaps and system defects and use their own knowledge in computer networks to carry out various attacks on network systems and information sources. Computer viruses have potential and unpredictable characteristics. If it is not prevented, the “time bomb” may destroy the entire network system of the local area network at any time. In the era of big data, the information security risk in the computer network is greater because it is more widely applied. Within the scope of data, both individuals and organizations rely heavily on data collection and analysis of big data. If the data is transferred or falsified, or the data is used to commit economic crimes, it may cause serious losses [2].

1.3. Application of big data technology in network security analysis

1.3.1. Big data technical analysis

Big data security analysis is mainly to optimize the shortcomings of traditional security analysis capabilities in network security analysis. The core technologies of big data technology include collection and processing, natural language understanding, traffic calculation engines, correlation analysis, large-scale machine learning, and visualization technologies. A variety of analysis methods, such as computer interaction, are the tool for quickly discovering security attacks and security threats in the ever-expanding massive amount of heterogeneous data information. In the big data technology security analysis, the technology is mainly analysed from distributed computing framework, computing streaming, computing engine, and distributed storage technology. Distributed computing framework does not rely on high-end hardware, and the advantages of strong scalability improve the adaptability of big data technology applications, so that some low-end devices can use this technology; streaming computing engine mainly solves the interaction of big data historical analysis system Formal computing provides convenient conditions for rapid search of network information and data; distributed storage technology can use multiple storage devices to share the storage load of large amounts of data, thereby expanding the storage capacity of big data technology and reducing storage management costs. To a certain extent, it also improves the reliability and security of the entire network security system.

1.3.2. The necessity of introducing big data technology into network security analysis

With the massive increase in the amount of network information data, the data sources are becoming more extensive and detailed, and the analysis dimensions are getting larger and larger. The use of traditional technical architecture and structured databases for data storage and analysis will not only increase, the storage cost of network information data will also cause part of the information data to be lost. Furthermore, as time goes by, some longer data cannot be stored well, which will bring difficulties to information and data tracking and searching in the future, and a wide range of data sources also brings great difficulties to the correlation analysis and fusion of heterogeneous data. It is difficult for traditional network security analysis technologies to meet the needs of huge and disparate network information data analysis [3].

The survey data conducted as early as 2013 shows that high-tech data processing has tremendous advantages in analysing and developing future information structures. A large number of data processing technologies can help to store and calculate quantities. Compared with traditional network security analysis methods, large-scale information technology can provide and promote network security. In developing countries, due to the lack of appropriate data collection and analysis systems, it is challengeable to collect, analyse data and obtain information quickly, which can improve the possibility of data extraction. Through the analysis of network security, it deepens and expands the analysis of network security, and lays a solid foundation for the wider network security analysis.
2. The main threats facing computer network security

2.1. Trojan horse
Trojan horse virus refers to the malicious code hidden in conventional programs, which has special functions, such as destroying and deleting files, sending passwords, attacking other special functions. Used for remote computer control, it will manage and control the parasite program in the computer system, and perform computer operations with other systems. The general Trojan horse virus program mainly focuses on finding the back door of the computer and using the server to steal passwords and important files. Trojan horse viruses are highly concealed and can suddenly launch attacks based on hackers' intentions.

2.2. Computer virus
Computer virus is a kind of potential program which is destructive, infectious that it destroys computer information or system. It may be hidden in other executable programs. Computer viruses can affect the speed of the machine, causing the system to crash. What's more, computer viruses can be classified into boot-type viruses, file-type viruses, and mixed-type viruses according to the existing media. They can be classified into source-type viruses, embedded viruses, and operating system-type viruses according to the link method. According to the system attacked, computer viruses is divided into viruses that attack DOS systems and viruses that attack UNIX systems [4].

2.3. Hacker attack
Hacking methods can be divided into two categories: destructive attacks and non-destructive attacks. The purpose of sabotage is to invade the computer system of others. Hackers use loopholes to damage the computer system, computer viruses, Trojan horse viruses and other hacker intrusions that seriously affect the normal operation of computer networks and even endangering national security. This is the main goal of protecting computer networks.

2.4. Software vulnerability
Because the design of computer software is current and limited, even though developers have enhanced their systems, there are still flaws. The software inevitably has certain flaws and vulnerabilities, which can be used by criminals to attack and control computers to steal important data and information from the computer, causing certain losses or troubles to the computer user.

Table 1. The characteristics of the main threats facing computer network security.

|              | Meaning characteristics                                                                 | Way of destruction                                                                 |
|--------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Trojan Horse | Malicious code with special functions                                                   | Destroy and delete files, send passwords, record keyboards and attack Dos          |
| computer virus | Code inserted in a computer program that destroys computer functions or data             | Destroy important computer data, consumes memory and disk space                   |
| hacker attack | Hackers use computer viruses, Trojan horse viruses to invade computer software systems  | Seriously affected the integrity of the computer network normal order, even endangering national security |
| Software vulnerability | The negligence of the software developer when developing the software, or the limitation of the programming language | Vulnerabilities are exploited to attack and control computers |
The software security problem in network application systems has always been a concern that plagues the development of the software industry. With the continuous increase in the number of applications, the continuous increase in complexity, and the continuous diversification of types, the difficulty of network security protection continues to increase. Comprehensive analysis illustrates that two major causes of security problems can be seen. Security threats are the external causes of software problems. In addition, security vulnerabilities are internal causes. The development of high-quality software systems is the fundamental countermeasure [5].

3. Safety system software development and design
With the rapid development of network technology, users have diverse experiences and needs. Faced with all kinds of network software, it is only possible to avoid dangers by doing a good job in fundamental security. In order to bring convenience to users, software often asks users to provide some data. This information can be stored on the network and can be easily stolen and leaked, which will have a negative impact on users. In addition to leaking information, the accompanying virus problem cannot be ignored. Viruses have hidden characteristics, and many companies or individuals cannot identify hidden viruses. In order to improve the level of computer information security, it is necessary to install security system software, cooperate with fire prevention technology to regularly check risk factors and network viruses; users can only install anti-virus software: detect the network environment, improve the security protection level of the computer network system, and strengthen the network system Protection, to prevent information leakage or theft, in order to achieve the protection effect of computer information security [6]. Anti-virus software must be updated regularly during use to combat new viruses or illegal intrusions and improve the timeliness and advancement of computer information security.

4. Conclusion
To sum up, in the era of the explosion of data and information and the rapid development of computer technology, while enjoying convenience, meanwhile, we are also taking the risk of network information security. It is necessary to deeply analyse the sources and characteristics of computer network information security risks, take advantage of the situation, formulate targeted countermeasures, strengthen computer network information security management, improve system security level, prevent the occurrence of various security risks and realize the security protection of computer network information.

Acknowledgements
1. 2017, Shandong Vocational Education &Teaching Reform Research Project "Research and Practice of Ideological &Political Teaching Effectiveness in Vocational Colleges Based on Big Data", project number: 20172774;

2. 2018, Humanities and Social Sciences Research Project of Shandong Colleges and Universities "Research on the Effectiveness Improvement of Ideological &Political Education in Colleges and
Universities in the Era of Big Data project number: J18RB035.

References
[1] Qu ye, Zhang Hao; Analysis of bug scam automatic static vulnerability detection [J]; Information security and communication security; 2007.
[2] National Information Security Standardization Technical Committee; Network security of information security technology Guidelines for the implementation of full level protection: GB / T 25058-2019 [S]; Beijing: China National Standard Press; 2019.
[3] Feng Kai; Construction and application of private cloud and big data training platform in Computer Experimental Centre [J]; Electronics World; 2018.
[4] Zhou Han; Analysis of computer network information security and protection strategy in the era of big data [J]; Digital age Jie; 2017.
[5] Zhang Linxia; Research on vulnerability detection method based on big data analysis [D]; Nanjing post and telecommunications University; 2017.
[6] Zhang Xiaohao; Discussion on information security assessment[J]; Information network security; 2012.