Computer Network Security Based on Prevention and Control of Network Virus

Wenya Zhu
Yiwu Industrial & Commercial College School of Mechatronics & IT, Yiwu, Zhejiang, China, 322000

*E-mail: 349504885@qq.com

Abstract. With the advent of the 21st century and the rapid development of science and technology, the concept of information technology (IT) penetrates into people's minds gradually. What's comes with it is the large-scale utilization of the network. It is exactly the development, continuous popularity and openness feature of the network that allow the extensive and fast spread of network virus, which has destroyed the connectivity of network resources. To solve this problem, the author explored the features of computer virus as well as the prevention and treatment to improve the computer cybersecurity.

Keywords: Network Virus, Computer, Security

1. Introduction

With the continuous deepening of science and technology and network communication technology, the society has gradually developed into the era of information explosion[1-2]. This era has the characteristics of digitization, networking, informatization and so on. The center of the era is computer network information[3-4]. Computer has developed into a necessity in human life and work, playing an important role. With the gradual informationization of society, the network improves people's work efficiency, enriches their spare time life, effectively improves the economic benefits of enterprises, and creates corresponding development opportunities. On the other hand, with the increasing number of network viruses, it is a great threat to the safe operation of computer network. Virus and virus analysis is a persistent work. They exist in each other. With the reform and development of computer technology, in order to effectively eliminate network virus, we must first analyze its causes and activity rules, so as to improve the computer network security technology, [5-6].

Currently, with the development of data centralization, computing centralization, and network complexity, the form of information security is becoming more and more serious. In the initial stage of network construction, companies often consider the applicability of business only, lacking the overall planning of security. As a result, the network is prone to security risks due to improper design, configuration, and application. Hence, for enterprises, how to continuously improve the information
security mechanism, ensure the security of system services, ensure the stability and normality of network and infrastructure, and prevent and control the risk of information security are the key issues to be solved. But just because of the popularity of the network, network virus, and computer cybersecurity have increasingly become hot issues. Hence, it is necessary to identify an effective solution to handle the network virus and ensure computer cybersecurity at this stage. To truly solve the network virus, we have to implement the features of network viruses to carry out targeted analysis and achieve the purpose of sustained computer security.

2. **Features of network virus**

The regulations of the people's Republic of China on the protection of computer system security clearly states that “a set of program codes that destroy computer functions or data, cause the computer to fail to operate normally, and can reproduce itself are called network virus”

1. Strong executive power. The programming principle of network virus is similar to that of legal application program, which can execute the commands in the program code. It is a micro application program. Compared with legal application program, it is incomplete, so it is mostly parasitic in files and source programs, and uses the execution power of legal program.

2. It is infectious and spreads fast. It can attack every object with the fastest speed. And once it is parasitic with a file or source program, it will continue to derive and copy, and make many destructive activities to achieve the purpose of self-replication.

3. It is latent. Generally speaking, the network virus will be similar to cancer after entering the computer system. It has a period of incubation period. It will be broken one by one and spread to other files slowly. It is difficult for people to find its existence. And it has certain concealment, which brings great threat to the safe operation of computer network.

4. It can be triggered. When a computer is operated improperly, it will induce related virus outbreak. Therefore, the standardized operation of computers can prevent the generation of viruses.

3. **Understanding of cybersecurity**

To make the software, hardware and related data in the network system fully maintained, to avoid the change of malicious network virus and the damage to the data leakage in the network equipment and the normal use of the system, it is necessary to fully understand the cybersecurity in the network service. Only by understanding the concept of cybersecurity can we better understand the network virus and network The relationship between cybersecurity.

Given the sample data set, \( D = \{ x_1, x_2, \ldots, x_n \} \), \( x_i \in \mathbb{R}^d \), \( i = 1, \ldots, n \). It is assumed that the first sample L is labeled as \( \mathbf{c} = ( x_1, x_2, \ldots, x_l ) \), and the corresponding label \( \mathbf{y} = ( y_1, y_2, \ldots, y_l ) \).

The significance of each feature dimension in the classification problem is different. To some extent, the computer cybersecurity data can overcome the shortcoming that the computer cybersecurity data treat each feature dimension equally. Its definition is as follows:

Sample \( x_i \) and \( x_j \) in the computer cybersecurity data are defined as follows

\[
d_d(x_i, x_j) = \sqrt{(x_i - x_j)^T A (x_i - x_j)},
\]

(1)

Where \( x_i \in \mathbb{R}^d \), \( A \in \mathbb{R}^{d \times d} \) represents symmetric semi positive definite matrix.

Based on the properties of semi positive definite matrix, the above equation can be written as follows:
\[
\begin{align*}
    d_d(x_i, x_j) &= \sqrt{(x_i - x_j) \tau A(x_i - x_j)} \\
    &= \sqrt{(x_i - x_j) \tau L L (x_i - x_j)} \\
    &= \sqrt{(Lx_i - Lx_j) \tau (Lx_i - Lx_j)}.
\end{align*}
\] 

(2)

It is equivalent to the matrix as a mapping, mapping the data of the original space to the new space, the computer cybersecurity data of the original space is transformed into the computer cybersecurity data of the new space. For cybersecurity, we explore from two aspects. On the one hand, from the aspect of information security, information security is mainly reflected in the integrity and availability of information preservation in the network. Unless permitted, it is not allowed to steal or peek the personal privacy and private number of the owner. On the other hand, from the perspective of system security, system security here refers to the integrity of the hardware of computers or other types of network devices used by the public.

4. Case analysis of computer network security

According to the relevant management system, the relevant departments shall define their own responsibility scope, implement and implement the responsibility system, adhere to the principle of "who manages, who is responsible" in the process of computer network and information security management, do a good job in preventive work, gradually form a systematic and perfect computer network security supervision system, strengthen system management, and introduce advanced management technology Security mechanism and authentication method of dynamic password are implemented. Generally speaking, the use of encryption technology can effectively protect the security of information. With the rapid development of computer network technology, password technology has changed a lot, especially digital password, identity recognition and fingerprint recognition system.

Given the increasing number of network viruses, the accelerating speed of transmission, and the elimination process is particularly difficult, it is necessary to not only prevent and avoid through human factors but also eliminate network viruses by practical technical means to provide a better technical guarantee for the use of computer security. After exploring the technical measures of network virus, it can be summarized as the following content, i.e., the use of virus prevention and control related software or firewall settings. To use the function of firewall well, first of all, we need to know what firewall is. Firewall is a technology to isolate the external network and the internal network in the maintenance of computer security. In this way, the control of information transmission and communication between the external network and the internal network can be implemented. According to the instructions required, we can reject the external network or allow the information transmission of the external network, making use of this kind of effective In short, if the instruction is given to allow the information to spread with the outside network, it can carry out effective information transmission. If it refuses to perform the information transmission of the outside network, it will block the information transmission.

With the iterative evolution of the network, the cybersecurity content has changed significantly. In the traditional network era, the content of cybersecurity is based on the physical stability of the network. In the cybersecurity nowadays, the transformation from the media to the carrier of national security, public security, and economic security has been completed. The shift of the focus of work and life to the online and the transition of the network space have been implemented. Layer presentation of cybersecurity content in the era of traditional network is shown as table 1.
Table 1. Layer presentation of cybersecurity content in the era of traditional network

| Times series            | Cybersecurity type | Cybersecurity content                        |
|-------------------------|--------------------|----------------------------------------------|
| Network 1.0 Era         | System security    | Illegal intrusion                            |
|                         | data security      | Illegal acquisition, theft and use          |
|                         | Application Security| Destroy application and software             |

In the era of artificial intelligence (AI), the legal interest of cybersecurity is not a single legal interest, but a compound legal interest. With the high dependence of the whole society on the network and the living of intelligent technology, paying attention to cybersecurity is to pay attention to national public security, public security and information security, which is also the logical starting point of studying cybersecurity. Layer presentation of cybersecurity content in the era of AI is shown as table 2.

Table 2. Layer presentation of cybersecurity content in the era of AI

| Times series     | Types of cybersecurity | Content of cybersecurity                      |
|------------------|-------------------------|------------------------------------------------|
| The age of AI    | Space Security          | National security, public security, economic security |

5. Conclusion
With the development of computer technology, in the process of network communication technology, the virus has been lurking in the hidden place. The emergence of network virus seriously threatens the safe operation of computer network, causes the leakage of network information and other phenomena, and causes great trouble to human life. Therefore, in order to improve the computer network security technology, it is necessary to formulate corresponding preventive measures against viruses, optimize the network working environment, and ensure the normal operation of the computer network, so as to promote the rapid development of the computer industry in China.

Acknowledgments
The 2020 scientific research project of Yiwu Industrial & Commercial College "Research on computer network security and prevention based on network virus attack". Funding number: ZD2020JD134-01.

References
[1] Yoon-Ho Choi, Moon-Young Jung, & Seung-Woo Seo. (2011). A fast pattern matching algorithm with multi-byte search unit for high-speed network security. Computer Communications, 34(14), 1750-1763.
[2] Manulis, M., Schneider, S., & Sadeghi, A. R. (2012). Applied cryptography and network security. Lecture Notes in Computer Science, 3089(7), 655-660.
[3] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng, & Xiaofeng Liao. (2013). Body area network security: a fuzzy attribute-based signcryption scheme. IEEE Journal on Selected Areas in Communications, 31(9), 37-46.
[4] Shetty, N., Schwartz, G., & Walrand, J. (2010). Can competitive insurers improve network security. Lecture Notes in Computer Science, 6101, 308-322.
[5] Alfaro, J. G., Coppens, F., Cuppensboulahia, N., & Preda, S. (2011). Mirage: a management tool for the analysis and deployment of network security policies. Lecture Notes in Computer Science, 6514, 203-215.
[6] Bimal Kumar Mishra , & Neha Keshri. (2013). Mathematical model on the transmission of worms in wireless sensor network. Applied Mathematical Modelling, 37(6), 4103 - 4111.