Pisco Med Publishing

Analysis on Network Security and Its Countermeasures

Qinghua Jiang,Lilin Lin,Yanhong He

Electronic Information Institute, Tonghua University of Science and Technology, Jilin, China

Abstract: With the rapid development of computer technology and the popularization of the network, human civilization is undergoing profound changes. The network has become an important resource for the political, economic, military and cultural aspects of the country and has become a symbol of national soft power. With the extensive use of computer networks and the increase in data transmission between networks, network security issues are becoming more prominent. Network security is related to national security, social stability, economic development and cultural construction and other fields, has become a hot topic of global concern. If a country cannot guarantee the security of network information in terms of collection, storage, transmission and authentication, it is impossible to obtain the efficiency and efficiency of information technology. The social and economic life is difficult to be carried out in a healthy and orderly manner. When the status of China's network information security is not optimistic. People should correctly deal with the negative impact caused by the process of information technology, take positive measures to protect the security of China's network information.

***Keywords*:** network, security, countermeasures

1. China's network security

1.1. Connotation of network security

The specific meaning of computer network security will change with the user changes, different users, the understanding of network security and requirements are different. For example, from an ordinary user's point of view, it may be that only personal privacy or confidential information is protected from being transmitted on the network, to avoid being eavesdropped, tampered with and forged; and the network provider, in addition to being concerned about the security of the network, Consider how to deal with sudden natural disasters, military attacks on the destruction of network hardware, and how to restore network traffic in the network, to maintain the continuity of network communications.

In essence, network security includes the hardware, software, and the security of the information on the network that make up the network system, so that it will not be damaged by accidental or malicious attacks. The network security has both technical problems and management side of the problem, the two sides complement each other, lack of a small can. Human network intrusion and aggression make network security face new challenges. The International Standardization Organization (ISO) defines 'computer security' as: 'the establishment and adoption of technical and regulatory safeguards for data processing systems, the protection of computer hardware, the failure of software data to be destroyed, tampered with by accidental and malicious leakage'. The definition of the above computer security, including physical security and logical security of both the contents of its logical security content can be understood as we often say that information security, refers to the confidentiality of information, integrity and availability of protection, and network security the implication of sex is the extension of information security, that is, network security is the protection of network information confidentiality, integrity and usability.

doi: 10.18282/ics.v1i1.588

At present, there are a variety of security vulnerabilities and threats in public data communication networks. Broadly speaking, all technologies and theories related to the confidentiality, completeness, usability, authenticity and controllability of information on the Internet are all areas of cybersecurity research.

1.2. Current status of China's current network security

According to the latest statistics, as of December 31, 2006, the total number of Internet users in China was 137 million, compared with the same period last year, the total number of Chinese internet users increased by 26 million a year, a growth rate of 23%. We can see that the total number of Internet users in China showed a rapid development trend. But the current use of the operating system and information processing chip hardware and software core technology almost always by foreign control, a variety of back door, security risks prevalent in recent years, computer system vulnerabilities found faster, large-scale worm attacks continue to erupt, so Posing a more serious challenge to our network security.

Computer viruses are increasingly rampant

The computer virus appeared in the late 1980s and originated in the United States. 1984 National Computer Security Conference demonstrated a computer virus test, put forward the 'virus' the term. After the 'Internet network incident' in 1988, began a large-scale anti-virus technology research. Statistics: There are tens of thousands of computer viruses are widely circulated around the world. The structure of the computer system itself causes the computer virus to produce, and the information sharing is the foundation and the means of the virus survival and the spread.

A computer virus is a program that modifies other programs by embedding itself into other programs. So, the essence of the virus is 'program', is a group can be executed, and must be executed by the order. It is a wide range, but also with infectious, hidden, sudden, destructive, has become the main killer of the urgency of security.

Threat of infectious viruses

The virus has a self-replicating feature, which replicates on an additional viral vector, as a new source of virus, which is mainly achieved through hard disks and networks. The infection is divided into three types: First, the operating system virus, it plays a destructive role in the boot block, its strong contagious, fast, large damage to the system can lead to system collapse. Second, the file virus, the virus itself can be copied to the executable file header or tail, only modify the contents of the program header register, change the order of the implementation of the program. Third, the source virus, the program is compiled before the virus into the program, together with the source code compiled into an executable file, such a virus hidden in the compiler, connect the program or editor.

Threat of concealed virus

Hidden virus work, you can impersonate the boot record, or nested in the implementation of the file into the memory, while the infection or damage, and caught in the normal file access, so that users are not easy to find the illegal operation of the virus.

1.3. Threat of sudden virus

When the conditions specified in the program are not met, the virus lurking in memory, disk files, once the specified conditions are met, the virus will be implemented immediately.

Threat of a devastating virus

Destructive virus in the process of infection and attack, the system and the system to destroy the file, and cause unimaginable consequences.

2. Hacker technology spread increasingly rampant

The word hacker is the beginning of the meaning of computer fans, and now refers to the computer network emergency system for unauthorized access to the staff, they can decipher the computer emergency system password, breaking the system security. Hackers attack a lot of means, through the network monitoring to obtain the user's account and password, key or authentication code, through the covert channel for illegal activities, damage to the firewall.

The threat of hacker attacks: hacker attacks than the history of the virus has a purpose, and thus history is dangerous. Currently known as hacking means up to more than 500 species.

August 8, 2006, according to the first letter of emergency safety blog 2,52 reported that scientists said the hacker life and 20 years. In the fifth 'Xing Wan light' youth academic annual meeting, the Chinese Academy of Sciences, University of Science and Technology of China

Professor GC. Guo said: 15 to 20 years later, a new computer that quantum computer will enter the application stage. By then, the computer will become very safe, the password is difficult to be stolen, clever 'hacker' will only be disappointed.

Computer crime cases increased year by year

Computer crime has created an unprecedented new threat to the world. Criminologists predict that the future forms of information social crime will be mainly computer cybercrime. China has been the first case of computer crime since Shenzhen in 1996. Computer crime has been rising from the line. The criminal means have also become technical and diversified. Crime is also expanding, many traditional forms of crime on the Internet can find the shadow, and its harm has far exceeded the traditional crime. Computer crime subjects mostly mastered the computer and network technology professionals and even the original computer and network technology and information security technology experts are also exposed to the risk of the use of the means of crime is more specialized. They are aware of the network of shortcomings and loopholes. Use rich computer and network technology, with a network of all directions, the network and a variety of electronic data, information and other information to attack, to destroy.

3. Network security countermeasures

3.1. Virus and hacker attacks prevention

Computer virus prevention refers to the virus has not yet invaded or just invaded, to intercept, block the virus intrusion or immediately alarm. The two opposing technologies of the virus are computer virus technology and anti-virus technology, they are based on programming technology, and its development is a spiral rise process, cannot be separated from the level. Users need to ensure that digital security needs from this

Several parties to consider: First, strengthen management, the establishment of the corresponding information security management system; Second, to adopt the most advanced information security technology; Third, improve the corresponding policy and legal system.

In the confrontation with the computer virus, first of all, should take effective defense measures, so that the system is not infected, to prevent the virus invasion than the virus after the invasion to find and exclude it important. The computer virus should be the main prevention, extensive publicity and education, improve the management, technical departments and users of the computer security and anti-virus knowledge level, increase immunity, resistance. Second, any kind of computer virus infection is achieved through a certain way. From the management measures to be taken seriously, can effectively prevent the virus infection. Reduce the virus cross-infection, blocking the virus infection is an effective way to prevent the invasion of the virus. In addition, but also with some anti-virus experts to maintain close contact in order to timely access to new virus control information

To ensure the safety of network information, the prevention of computer viruses and hacker attacks, in the specific implementation of the following different types, to take specific preventive measures.

Operating system type virus

Prevent the operating system virus: First, modify the interrupt service routine, increase the system on the hard disk boot sector check function, early detection of the invasion of the boot sector virus. First, after the implementation of the disk (hard disk) to lock the program, the machine before the implementation of the lock program, so that even if the virus in the boot area can also be covered by the original content.

The implementation of the implementation of the letter h, file type virus

Preventive execution information file-based viruses are transmitted through executable information files, thus ensuring that the integrity of the executable information files can be prevented. In order to prevent the executable emergency file from being modified or to detect whether it has been modified, the information file is encrypted and the encryption method is legal. Encryption method: the implementation of the file is encrypted after the encryption into the system, when the run-time by the decryption system, and then run. If the operation fails, the executable information file has been modified since it was encrypted. Encryption method is legal: the user key and information files interact with each other, by testing the secret effect and in the same time before and after the same time to detect the information integrity of the file, such as the results of two different tests, this information file has been modifying.

Protection interrupt vector table

When the virus stationed in memory, you need to modify some of the interrupt vector, therefore, the interrupt vector table recovery is necessary, the reader set up a correct interrupt vector table backup, through the comparison of the interrupt vector table to find whether there are abnormal interrupt vector changes.

Timely installation of anti-virus card, anti-virus software

Virus intrusion system, some users do not often use the operation, such as directly modify the boot sector, file partition table, directory table, operating system files, interrupt vector table, Shen Hua memory space and stationed, so the reader can have direct access to the system as a restricted area, to prevent their direct reference, so to limit the virus invasion. Such as the choice of safe popular network firewall software, it can immediately monitor the page on the insecurity, in case of no registered procedures will be security warning, may block some commonly used software, such as cannot enter the joint or not on the QQ and so on. To prevent the danger of the Internet (viruses, resource theft, etc.) spread to the computer.

Pay attention to the security of information sharing on the LAN

Cut off the way the virus spread, it is recommended to cancel unnecessary sharing. Set the password and read-only in the shared info file. If it is not read-only, then the virus on the network to write the reader's computer will be easier, the password can also effectively protect the reader's information is not easily accessible to others.

To control the virus infection is the focus of anti-virus

The key to anti-virus is the judgment of the rus behavior, how to effectively identify the virus behavior and normal program behavior is an important factor in the success of anti-virus. The difficulty of anti-virus is how quickly, accurately and effectively identify the virus, improper handling will bring 'false alarm', like 'wolf' allegory, the consequences of frequent false alarm is no longer cause the police alert. In addition, anti-virus for the virus mechanism is not designed according to the existing virus may also be powerless, such as in the DIR2 virus before the advent of anti-virus software or anti-virus card, almost no one can control the virus, the reason lies in the virus mechanism has been beyond the scope of the anti-virus software and anti-virus card. Today, the mechanism of the virus has been recognized, is the new anti-virus software and anti-virus card, you can control the virus and its variants of the virus.

To ensure the safety of information --- concerned about the popular virus and download the killing tool

Because there are many popular viruses and special viruses, to prevent the expansion of the virus, a lot of anti-virus software vendors and the official website free to provide the killing tool. Some viruses use ordinary anti-virus software or not, need to kill tools, cut off the way the virus spread. Therefore, the need to always pay attention to the official website, announced a new type of virus and download the corresponding killing tool, so that the first defense is better.

In order to ensure the security of the information, the user should note: If the file is lost, damaged and the system cannot start the normal phenomenon, should turn off the computer, to avoid losing more data; e-mail processing should be cautious, in addition to their own sources of information can be open, but the e-mail attachment procedures do not run lightly, you can first apply anti-virus software and professional removal of Trojan virus tools, scan and then use; in the use of chat software, their IP address is best not to leak, to prevent hackers.

Timely data backup

The emergence of the virus is unpredictable, and anti-virus software is not necessarily guaranteed to kill all the virus, the user data to do a timely backup to ensure the safety of information. In addition, the backup of the personal data generally takes up less space, the use of mobile disk storage is convenient and safe. But in the backup of various information and information, it should be determined at the same time without virus, or mobile disk is also difficult to prevent the virus cross-infection.

The virus and the system 'loopholes' to prevent

To install patches frequently, antivirus software, firewall upgrades in a timely manner to develop a series of security policies, including LAN users access to the Internet authentication and access strategy. To prevent external attacks, always check the security of the network, view the firewall log. Tracking the development of network virus prevention and control technology, can be used effective new technology, new means, the establishment of 'to prevent the main to kill as a supplement, anti-kill combination, hardware and software complementary, tackling the problem, comprehensive management' network virus Safe mode.

To prevent hackers

On the use of the computer network to implement effective monitoring means to seize the attackers; First, the use of network security scanning system to find hackers invasion; Second, the use of the latest anti-kill software to prevent hacker attacks; Fourth, the use of expert systems to repair the system being attacked.

4. Conclusion

Our government is trying to construct a comprehensive legal framework of information, to a certain extent, solve the problem of our network that cannot be solved, but to protect the long-term national information security, complexity is still in its infancy. The nature of the network determines the characteristics of network security law, status and network security technology, and therefore in the study of legal protection must consider its technical characteristics, in line with technical requirements. In view of the development of network technology and the imbalance of security protection, it is necessary to establish a laws and regulations from technology to law, from hardware to software, from import to export, from facility to information content, to all walks of life, departmental laws and regulations for the warp of China 's network information security 'law'.

References

1. XW Zhou, editor. Information network and security. Defense Industry Press, January 2006.
2. N. Ju. Information Security - Protection of the Internet World. Military Science Press, January 2003.
3. SW Deng. Network environment, digital library security and preventive measures. 'Library Forum', 2004 No. 8.
4. PG Li, SJ Zhong. Digital library information security issues and related countermeasures. Modern Newspaper. 2005 the ninth period.
5. RX Fu, L Ma. Hacking crime in the field of e-commerce. Network Security Technology and Application. 2006 the second period.
6. Y Zhang. On network security. Journal of Changchun University. 2006 the second period.