New Trends in Network Security and Precautions

Jun Xiang

Security Bureau, Enyang District Committee, Bazhong Province, Sichuan Province, Bazhong 636064

Abstract: ***With the continuous development of network information technology in China, the incidence of computer network security problems is also getting higher and higher. Once the computer appears network security problems will directly affect people's normal life and production. Therefore, computer users need to have a strong awareness of network security management, take effective measures to prevent computer network security problems, and reduce the incidence of computer network security problems.***

Keywords: Computer; Network security; Problems; Precautions.

1. OVERVIEW OF COMPUTER NETWORK SECURITY

(1) Has strong confidentiality

Effective security guarantees can be provided for users' personal information in the online environment.

(2) The speed of data information dissemination is faster

The dissemination of data information on the internet is not affected by time and geography, and can expand the scope of information dissemination in the shortest possible time. It is precisely based on the above characteristics that there is a greater need to strengthen effective management of computer network security and improve the security and stability of computer network systems.

Recent researches encompasses a wide range of research topics, including supply chain management, digitization, clinical trials, federated learning, network orchestration, legal text classification, automated surveillance, conversational agents, financial forecasting, green innovation, object detection, autonomous navigation, image fusion, and real-time data processing.

Liu et al. (2024) examine the impact of supply chains and digitization on the development of environmental technologies, considering the roles of inflation and consumption in G7 nations. Li (2025) focuses on optimizing clinical trial strategies for anti-HER2 drugs using Bayesian optimization and deep learning. Huang et al. (2024a) explore the contribution of federated learning to trustworthy and responsible artificial intelligence, while Huang et al. (2024b) investigate a multi-agency collaboration system for medical image analysis and classification based on federated learning.

In the field of network security and orchestration, Liang and Chen (2019a) propose a SDN-based hierarchical authentication mechanism for IPv6 addresses, and Liang and Chen (2019b) introduce HDSO, a high-performance dynamic service orchestration algorithm for hybrid NFV networks. Xie et al. (2024) advance legal citation text classification using a Conv1D-based approach, and Xu et al. (2024a) develop a real-time detection system for crown-of-thorns starfish using YOLOv5 deep learning. Xu et al. (2024b) enhance user experience and trust in advanced LLM-based conversational agents.

Liu (2024) optimizes supply chain efficiency using cross-efficiency analysis and inverse DEA models. Bi et al. (2024) discuss the role of AI in financial forecasting, focusing on the potential and challenges of ChatGPT. Yan et al. (2024) analyze the impact of CEO power on manufacturing firms' green innovation and organizational performance through a mediational approach. Chen et al. (2022) present a one-stage object referring method with gaze estimation.

Wang et al. (2024) research autonomous robot navigation based on reinforcement learning, and Wu et al. (2024) propose a lightweight GAN-based image fusion algorithm for visible and infrared images. Zheng Ren (2024a) introduces a novel approach for role-oriented dialogue summarization, and Z. Ren (2024b) enhances Seq2Seq models for role-oriented dialogue summary generation through adaptive feature weighting and dynamic statistical conditioning. Fan et al. (2024) optimize real-time data processing in high-frequency trading algorithms using machine learning.

2. PROBLEMS FACED BY COMPUTER NETWORK SECURITY

2.1 Invasion of Computer Viruses

Usually, computer viruses lurk within computer programs, and criminals can cause serious impact and damage to computer and network system security by writing virus programs. Once a virus invades, the information and related programs in the computer system are easily maliciously stolen, destroyed, and copied, and in severe cases, can cause serious system crashes. Computer viruses have strong concealment, infectivity, and parasitism, and are usually spread through local area network sharing and network media, making it difficult to completely eliminate them.

2.2 Threats of Computer Network Vulnerabilities

Microsoft software is currently the most widely used computer system by computer users. However, pirated Microsoft software is constantly emerging on the market, posing numerous vulnerabilities to computer networks and posing a great threat to network security. In an open network environment, if users engage in non-standard browsing behavior, it is easy for viruses to enter the computer and attack the internal system, resulting in numerous computer vulnerabilities and threatening the security of the entire network system.

2.3 Violations by Computer Users

The illegal operations of computer users are also an important cause of computer network security issues. According to the survey, the majority of computer users in China have poor awareness of data security, lack professional knowledge of computer operations, and lack understanding of computer security protection theory and technology, resulting in behaviors such as browsing web pages, commenting, liking, and forwarding information at will during computer operations. If a user browses a webpage containing viruses, it will open the door to the invasion of network viruses and cause significant computer network security issues. The threat of spyware and spam emails is that computer networks have strong openness, and many data information are interconnected, which creates conditions for illegal personnel to invade. Some illegal individuals may use spam emails to spread network viruses. Computer users may inadvertently authorize the use of these spam emails. Once these viruses are opened, they will invade the entire computer network. At this time, illegal personnel will steal or tamper with important data, and stealing users' personal privacy will have a serious impact on the computer network system.

2.4 Network Hacker Attacks

Network hackers refer to attackers who illegally access and damage users' networks through the internet. Hackers can peek into others' privacy and manipulate or destroy users' information in various ways. Therefore, the uncertainty of hacker motives has a significant impact on users' interests and security. If hackers only pry into users' privacy out of curiosity and do not damage their network systems, although the harm to them is relatively small, it still causes certain harm to users. If hackers have malicious intentions to damage users' network systems, the consequences would be unimaginable. For example, some hackers may attack users' target web pages and content, which can cause network paralysis and prevent users from using them normally, posing a great threat to their own interests; Some hackers have negative emotions, such as malicious attacks and destructive psychology, tampering and destroying important data information in users' computers. In severe cases, it may pose a threat to national defense, military, economic, political and other confidential intelligence, putting national security at the center of public criticism.

2.5 Computer hardware facility failure

Computer hardware configuration failures can also cause corresponding network security issues. If the staff does not regularly maintain and upkeep the computer hardware settings, once some hardware facilities fail, it will interfere with the normal operation of the entire network system, not only reducing the speed of computer operation, but also causing incomplete display of some important information.

3. PREVENTIVE MEASURES FOR COMPUTER NETWORK SECURITY

3.1 Enhance awareness of computer network security prevention

After using the computer, computer users should promptly clear the private information in the computer, encrypt the information in the computer, and prevent personal information from being leaked on public computers. Personal ID information, photos, home addresses, etc. cannot be exposed on the internet at will to prevent inconvenience to oneself. If someone encounters a website that may have problems while surfing the internet, do not click on it casually to prevent viruses from entering the computer system. When using a computer, a firewall should be installed, and vulnerabilities and patches in the system should be regularly checked to reduce the impact of computer viruses and vulnerabilities on computer security.

Government departments and enterprises should cultivate talents in computer network security when preventing computer network security issues, and jointly establish talent training mechanisms with universities to develop efficient network security protection methods, in order to reduce the threats posed by hackers, viruses, and other threats to computer networks. Especially in key units and enterprises, computers contain a large amount of important information and files. When using computers, it is necessary to enhance awareness of network security protection and take effective protective measures to reduce the threat of viruses and other threats to computer systems.

3.2 Installing Computer Security Protection Software

Installing security protection software is an effective measure to ensure the security of computer networks, which can greatly improve the security of computer network systems. Security protection software can effectively prevent viruses from affecting computer network systems as before. Once a network virus invades a computer system, the functions of security protection software will quickly start, filter and intercept network viruses, achieving real-time health and protection of the entire computer network environment. Security protection software can monitor and control virus information in computer network systems. Once a network virus maliciously changes the data in the computer system, the security protection software will pop up as soon as possible, reminding users to pay attention to scanning and killing computer network viruses to ensure the security of computer network data information.

3.3 Timely installation of vulnerability patches

With the continuous development of modern science and technology in our country, computer hardware settings have become increasingly sophisticated.

The types and functions of software are becoming more comprehensive, and computers often receive prompts for installing patches and system updates. If computer users ignore these update prompts, it is difficult to install patches and update the system in a timely manner, which can easily lead to corresponding vulnerabilities in the computer network. To address this issue, computer users can download corresponding virus scanning and security protection software from the official website, among which Rising Antivirus and 360 Security Guard are the most common virus scanning and security protection software. This type of software can ensure the security of the computer system to the greatest extent possible.

3.4 Regularly backing up important computer files

Computer users should develop the habit of regularly backing up their computer files, especially important file materials, which should be stored regularly. Hackers and computer virus attacks have strong randomness, and their attack methods, attack times, and other uncertainties are the biggest security threats to computer network systems. Developing the habit of regularly backing up important computer files and minimizing the leakage of critical information is of great significance for maintaining the security and stability of computer network systems. Computer users backup important files to other hard disk devices and save them, so that even if the computer network is maliciously attacked, there will be no problem of important data loss, effectively ensuring the security of user data information.

3.5 Use of data encryption technology

This technology can encrypt data information in computer networks, minimizing the problem of data theft and tampering, and ensuring the security of data transmission in computer networks. Data encryption technology includes various types, such as plaintext data encryption technology, ciphertext data encryption technology, key data encryption technology, encryption algorithm technology, etc. The most important and critical technology in data encryption is key encryption technology, which can ensure the security and privacy of computer network data information, effectively prevent illegal personnel and malicious software from tampering and stealing data information, and greatly protect the legitimate interests of third-party users. As one of the data encryption technologies, data signature technology can ensure the security of information transmission on the Internet. Data signature technology can effectively prevent external forces from stealing network data information. Digital signature technology can be applied in various stages of data transmission. Users can use secure passwords to protect important computer network data information, ensure the security of data information throughout the entire computer network transmission process, and safeguard the legitimate rights and interests of users.

3.6 Strengthen network system monitoring

In the process of network system operation, various illegal intrusion phenomena occur from time to time. If not detected in a timely manner, it will lay hidden dangers to the security of the network system and cause incalculable losses.

To effectively address some security risks in computer networks, monitoring of network systems is essential. Intrusion detection belongs to comprehensive protection technology, which analyzes and monitors the real-time operation status of the network communication monitoring system to timely detect illegal intrusion phenomena that occur in the network system. In the process of regulating network systems, signature and statistical analysis will be conducted to more effectively address potential security issues and provide protection for network security by monitoring network system vulnerabilities and conducting statistical analysis of network system operation status.

3.7 Strengthen the maintenance of computer hardware facilities

Staff should regularly strengthen the maintenance and upkeep of computer hardware settings to prevent line failures and component damage from hindering the normal operation of the host, and to improve the security and stability of computer networks. Computer users should avoid external interference with the network, and avoid placing their computers in damp and static environments to prevent external factors from interfering with the safe operation of the computer network.

3.8 Network Firewall Settings

Effective application of network firewalls can provide effective protection against malicious attacks from the outside world, as well as constrain the access of internal users to websites with security risks. If the enterprise's internal computer system is connected to the Internet, network security issues need not only to effectively resist viruses, but also to prevent system vulnerabilities. In addition, it is important to pay attention to the prevention of hackers, as network firewalls can take strict preventive measures against malicious intrusions from external networks. On this basis, it is necessary to reasonably divide the internal network of the enterprise and minimize the impact of security issues on the internal network of the enterprise. The setting of firewalls can closely monitor and audit the process of network information transmission and reading, and record all access records in detail. Based on this, corresponding access logs can be generated, which can provide powerful reference for subsequent network security maintenance work. Once there is a network security issue, the firewall can issue an alert in the first time, and also provide the type of problem and related handling suggestions.

4. CONCLUSION

At present, there are mainly system vulnerabilities, computer viruses, and information leaks in computer network systems, which pose a threat to the stability of the system and the security of data information. Therefore, in order to further improve the security of computer networks, it is necessary to enhance users' awareness of security precautions, introduce security protection technologies, strengthen monitoring of network systems, and effectively ensure the security and stability of network systems.

REFERENCES

[1] Wei Wang Analysis of Computer Network Security Issues and Preventive Measures [J]. Wireless Internet Technology, 2021, 18 (3): 37-38

[2] Ying Zhang Computer Network Security Issues and Preventive Measures [J]. Boutique, 2021 (4): 246

[3] Peiru Yan Preliminary Exploration of Computer Network Security Issues and Preventive Measures [J]. China Broadband, 2021 (2): 17

[4] Zun Li Analysis of Computer Network Security Issues and Preventive Measures [J]. Wireless Internet Technology, 2021, 18 (6): 28-29

[5] Liu, H., Li, N., Zhao, S., Xue, P., Zhu, C., & He, Y. (2024). The impact of supply chain and digitization on the development of environmental technologies: Unveiling the role of inflation and consumption in G7 nations. Energy Economics, 108165.

[6] Li, T. (2025). Optimization of Clinical Trial Strategies for Anti-HER2 Drugs Based on Bayesian Optimization and Deep Learning.

[7] Huang, S., Liang, Y., Shen, F., & Gao, F. (2024, July). Research on Federated Learning's Contribution to Trustworthy and Responsible Artificial Intelligence. In Proceedings of the 2024 3rd International Symposium on Robotics, Artificial Intelligence and Information Engineering (pp. 125-129).

[8] Huang, S., Diao, S., Wan, Y., & Song, C. (2024, August). Research on multi-agency collaboration medical images analysis and classification system based on federated learning. In Proceedings of the 2024 International Conference on Biomedicine and Intelligent Technology (pp. 40-44).

[9] Liang, X., & Chen, H. (2019, July). A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 225-225). IEEE.

[10] Liang, X., & Chen, H. (2019, August). HDSO: A High-Performance Dynamic Service Orchestration Algorithm in Hybrid NFV Networks. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 782-787). IEEE.

[11] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15–22. https://doi.org/10.53469/jtpes.2024.04(02).03

[12] Xu, G., Xie, Y., Luo, Y., Yin, Y., Li, Z., & Wei, Z. (2024). Advancing Automated Surveillance: Real-Time Detection of Crown-of-Thorns Starfish via YOLOv5 Deep Learning. Journal of Theory and Practice of Engineering Science, 4(06), 1–10. https://doi.org/10.53469/jtpes.2024.04(06).01

[13] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467

[14] Liu, M. (2024). Optimizing Supply Chain Efficiency Using Cross-Efficiency Analysis and Inverse DEA Models.

[15] Bi, S., Deng, T., & Xiao, J. (2024). The Role of AI in Financial Forecasting: ChatGPT's Potential and Challenges. arXiv preprint arXiv:2411.13562.

[16] Yan, Q., Yan, J., Zhang, D., Bi, S., Tian, Y., Mubeen, R., & Abbas, J. (2024). Does CEO power affect manufacturing firms' green innovation and organizational performance? A mediational approach. Sustainability, 16(14), 6015.

[17] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[18] Wang, Z., Yan, H., Wang, Z., Xu, Z., Wu, Z., & Wang, Y. (2024, July). Research on autonomous robots navigation based on reinforcement learning. In 2024 3rd International Conference on Robotics, Artificial Intelligence and Intelligent Control (RAIIC) (pp. 78-81). IEEE.

[19] Wu, Z., Chen, J., Tan, L., Gong, H., Zhou, Y., & Shi, G. (2024, September). A lightweight GAN-based image fusion algorithm for visible and infrared images. In 2024 4th International Conference on Computer Science and Blockchain (CCSB) (pp. 466-470). IEEE.

[20] Zheng Ren, "Balancing role contributions: a novel approach for role-oriented dialogue summarization," Proc. SPIE 13259, International Conference on Automation Control, Algorithm, and Intelligent Bionics (ACAIB 2024), 1325920 (4 September 2024); https://doi.org/10.1117/12.3039616

[21] Z. Ren, "Enhancing Seq2Seq Models for Role-Oriented Dialogue Summary Generation Through Adaptive Feature Weighting and Dynamic Statistical Conditioninge," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 497-501, doi: 10.1109/CISCE62493.2024.10653360.

[22] Fan, Y., Hu, Z., Fu, L., Cheng, Y., Wang, L., & Wang, Y. (2024). Research on Optimizing Real-Time Data Processing in High-Frequency Trading Algorithms using Machine Learning. arXiv preprint arXiv:2412.01062.

Author Profile

Jun Xiang male, born in 1982, of Han ethnicity, from Bazhong City, Sichuan Province. He holds a bachelor's degree and is a statistician. He is also a librarian specializing in archives at Sichuan University of Arts and Sciences.