Tech Science Press

check for updates

Analysis of Campus Network Security

Han Chu, Haoliang Lan*, Jie Xu and Xiao Feng Sun

Department of Computer Information and Network Security, Jiangsu Police Institute, Nanjing, 210000, China
*Corresponding Author: Haoliang Lan. Email: lanhaoliang@jspi.cn
Received: 28 July 2022; Accepted: 22 October 2022

Abstract: Campus network provides a critical stage to student service and campus administration, which assumes a paramount part in the strategy of 'Rejuvenating the Country through Science and Education' and 'Revitalizing China through Talented Persons'. However, with the rapid development and continuous expansion of campus network, network security needs to be an essential issue that could not be overlooked in campus network construction. In order to ensure the normal operation of various functions of the campus network, the security risk level of the campus network is supposed to be controlled within a reasonable range at any moment. Through literature research, theory analysis and other methods, this paper systematically combs the research on campus network security at home and abroad, analyzing and researching the campus network security issues from a theoretical perspective. A series of efficient solutions accordingly were also put forward.

Keywords: Internet; campus network; network security; protective measures

1 Introduction

With the advancement and development of modern science and technology, we have stepped into the digital age. Digital education have gradually become the main direction of educational development. However, network security is also threatened unprecedentedly. The campus network with a considerable number of users has become the target of many criminals. Network security has attracted more and more attention of the country and society, but the attack and prevention technology of computer virus is also expanding, updating and improving. At present, there are a large number of relevant studies on "network security" at home and abroad and the system is relatively mature, but most of them focus on aspects of traditional technology such as vulnerability scanning and firewall construction, lacking of relevant research on "campus network security" and analysis on "early prevention" of intrusion and relevant legislation. The main significance of this paper is: firstly, it introduces the concept and characteristics of "campus network"; Secondly, it deeply analyzes the sources of "problems of campus network security"; Finally, in order to provide guidance on the security construction of campus network, a series of effective measures accordingly are put forward, which enriches the traditional solution.

2 Overview of Related Research

2.1 Data Resources

In order to get further fathoms of the research status, we searched the topic through "Web of Science" with the keywords "network security" and "campus network security". By October 30, 2021, 282183 related articles of "network security" in English and 1285 related articles of "campus network security" in English (broad-based search) have been searched. Through the theme retrieval of "China National Knowledge Infrastructure" with the same keywords "network security" and "campus network security", 22700 documents related to "network security" in Chinese and 1896 documents related to "campus network security" in Chinese were finally obtained.

2.2 Time Distribution on Number Basis

Although the prevention technology of network security in China started late, it has developed rapidly. To some degree, the development of campus network represents the development of domestic Internet. Therefore, campus network security is a hot research object of many institutions and scholars. The research on campus network security in China began in 1997 (only one document), and then up to 2009, the research results showed an increasing trend year by year; Since 2010, the growth trend has been sluggish or even downward (as shown in the Fig. 1).
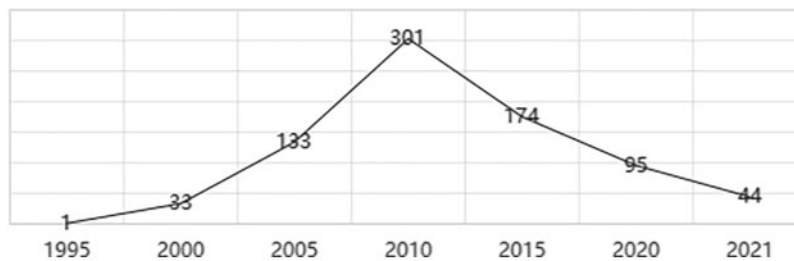
Figure 1: Times distribution of domestic papers

As is shown that some achievements of campus network security has been gained in China, but has been gradually ignored in recent years.

2.3 Important Papers at Home and Abroad

As is shown in Table 1, a portion of researches on campus network security were completed at home and abroad, enriching the relatively mature system of theory.

Table 1: Important papers

Number	Subject	First author	Time
1	Analysis and protection of computer network security issues [1]	Ju Jinquan	2020
2	Assessing the security of campus networks: The case of seven universities [2]	Rui Zheng	2021
3	Detection and prevention of network intrusion [3]	Zhang Bing-yi	2002
4	Analysis of computer network security [4]	Peng sha-sha	2012
5	Survey of network security awareness [5]	Gong Jian	2016

(Continued)

Table 1: Continued

Number	Subject	First author	Time
6	Problem and policy of security system in campus network [6]	Zha Gui-ting	2005
7	Awareness about the online security threat and ways to secure the youths [7]	Y. Nidup	2021
8	Assessing user's susceptibility and awareness of cybersecurity threat [8]	M. M. Althobaiti	2021
9	Research on the construction of network security governance system in campus [9]	Wei Chuyuan	2021
10	Managing delivery of safeguarding substances as a mitigation against outbreaks of pandemics [10]	S. A. Hassan	2021
11	Smart contract: security and privacy	L. S. Alotaibi	2021
12	A robust 3-D medical watermarking based on wavelet transform for data protection	X. R. Zhang	2022

Analysis and Protection of Computer Network Security Issues [1] were jointly completed by Ju Jinquan, a master's student at Soochow University in Korea, and two Indian students. The sources of network security problem were analyzed in this paper from the four aspects of network hardware, network software, network producers and users. It especially points out that the current construction of campus network mostly concentrates on the large-scale and overall development, ignoring the security construction.

So as to fathom the current situation of campus network security in China, the paper Assessing the Security of Campus Networks: The Case of Seven Universities [2] investigates the campus networks of seven universities in South China, including Wuhan University (WHU), Huazhong University of science and technology, China University of Geosciences (CUG), central China Normal University (CNUU), central China Agricultural University (HZAU), etc. According to the topological characteristics of campus network, a tool integrating network asset detection, network compliance audit and vulnerability matching-WebHunt were developed. With the help of WebHunt, many network security risks of seven universities were found (as shown in the Table 2). These network security issues were reported to universities and received positive responses. Even these domestic colleges and universities with top-level domain names in CERNET have so many security problems, which reminds the managers of campus network of campus that network security is the top priority of campus network construction that could not be overlooked.

"Analysis of Computer Network Security" [4] was published in 2012, when was the peak of the papers increasing in the field. And the paper was cited 168 times, which has great significance of practical reference for studying network security. Starting with the analysis of the causes of network security, the author Peng Sha-sha and her team, who are from the Air Force Engineering University, ends with network security defense with the help of firewall, Intrusion Detection System, data encryption and other technologies. It also puts forward that we need to improve the relevant legislation of network security, which adds new content and provides theoretical and technical support for network security defense.

Table 2: Security risk of report of seven universities

Security risk	WHU	HUST	CCNU	CUG	HZAU	ZUEL	WHUT
Zombie url	√	√	√	√	√	√	√
Domain name access error	√	√	√	√	√	√	√
Cname record	√	√	√	√	√	√	√
LAN IP leakage	√	-	√	√	-	√	-
Domain name resolution disorder	√	√	√	√	√	√	√
Subdomain name non-compliance	√	-	-	-	-	-	-
Port open abnormal	√	-	√	-	-	-	√
CVE vulnerability	√	√	√	√	√	√	√

Gong Jian, director of China Education and Research Network in East (North) China, is the core author in the field of network security. Survey of Network Security Situation Awareness [5] is a core review paper published by Professor Gong in 2016, which has been cited 192 times. This paper describes the new concept "Network Security Situation Awareness" again, and discusses the current hot issues of network security situation. A series of theory-based models provide strong support for the relevant research of network security situation awareness, and inspire the coping strategies of network security problems.

Guiting Zha, once professor of Nanjing Agricultural University, has made active efforts and outstanding achievements in the construction of CERNET for many years. Because his job is related to the management of campus, the author published the paper Problem and Policy of Security System in Campus Network [6] as early as 2005. Through investigation, the truth that 80% of computer viruses spread through e-mail was pointed out, inspiring experts to strengthen the protection of e-mail. Through system research and analysis, the loopholes in Windows and UNIX systems as well as the security hidden dangers in system configuration were pointed out. He put forward that if we want to establish safe and operational campus network, we would not only expected to establish a secure e-mail service system, centralized computer system of virus prevention and firewall, but also patch up system vulnerabilities in time.

2.4 Summary of Research Overview

Overall, a portion of achievements of the research in the field of network security has been gained, and the framework is relatively mature. Nonetheless, there is a relative absence of research on campus network security, and the relevant research has stagnated in recent years, lacking of representative literature. The coping strategies basically concentrate on the traditional technical aspects such as vulnerability repair and firewall construction. This paper will refer to and summarize pertinent papers, starting with the concept and characteristics of campus network, dissecting the source of campus network security problems, and put forward relevant countermeasures for the short board effect of security problems [11], that is, the safety effect relies on the weakest side. We should not best pay attention to improving the technical level, but also start from early prevention, perceive the network security situation, and strengthen the training of network security managers. Further, we are supposed

to improve legislation related to network security and strengthen supervision. Only in this way can we raise a safe yard for campus network and escort talent training,
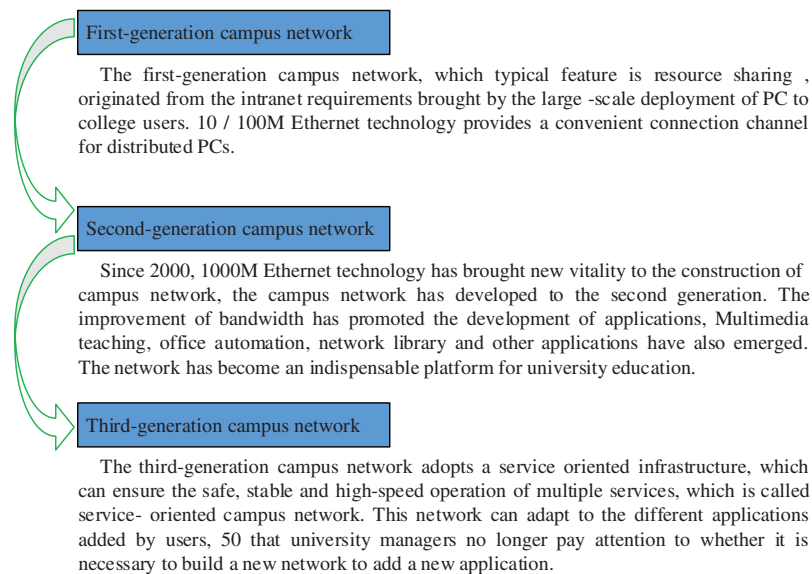
3 Concept and Characteristics of Campus Network

3.1 Concept of Campus Network

Campus network is defined as a computer network that provides resource sharing, information exchange and collaborative work for school teaching, scientific research and management under the guidance of clear educational ideas and theories [12].

3.2 Developments of Campus Network

Since the China Education and Research Network has been established in 1994, campus network has experienced rapid development for more than 20 years (as shown in Fig. 2), which represents the current situation of China's Internet development to a certain degree [13].

First-generation campus network

The first-generation campus network, which typical feature is resource sharing , originated from the intranet requirements brought by the large -scale deployment of PC to college users. 10 / 100M Ethernet technology provides a convenient connection channel for distributed PCs.

Second-generation campus network

Since 2000, 1000M Ethernet technology has brought new vitality to the construction of campus network, the campus network has developed to the second generation. The improvement of bandwidth has promoted the development of applications, Multimedia teaching, office automation, network library and other applications have also emerged. The network has become an indispensable platform for university education.

Third-generation campus network

The third-generation campus network adopts a service oriented infrastructure, which can ensure the safe, stable and high-speed operation of multiple services, which is called service- oriented campus network. This network can adapt to the different applications added by users, 50 that university managers no longer pay attention to whether it is necessary to build a new network to add a new application.

**Figure 2:** Developments of campus network

3.3 Characteristics of Campus Network

3.3.1 Environmental Distribution of Campus Network

After constantly development in more than twenty years, campus network is divided into seven areas according to the using environment (as shown in Fig. 3).

(1) Core region of network service. Including internal service publishing area and external service publishing area.

(2) Private network. Including financial network, One Card Solution network, security monitoring network and other private networks. In the same campus, different private network equipment connect directly through optical fiber; between different campuses, private network connection is relied on the leased operator's bare optical fiber link.

(3) Teaching area. Including ordinary classroom and computer classrooms with intensive computers, which requires reliable network quality, and generally adopts wired network.

(4) Offices. It requires the combination of wired network and wireless network, including offices of teachers and leaders.

(5) Public area. Including auditorium, library, canteen and other crowded public areas.

(6) Students' dormitory. It requires the combination of wired network and wireless network because students surf the Internet at some specific time. Campus network for most schools are paid for use, so they would also expected to concentrate on the anti-agent function.

(7) Family residence. Most of the residential areas of faculty require paid access to the network. At home, you can use the router to build your own Wife to meet the Internet needs of multiple terminals [14].
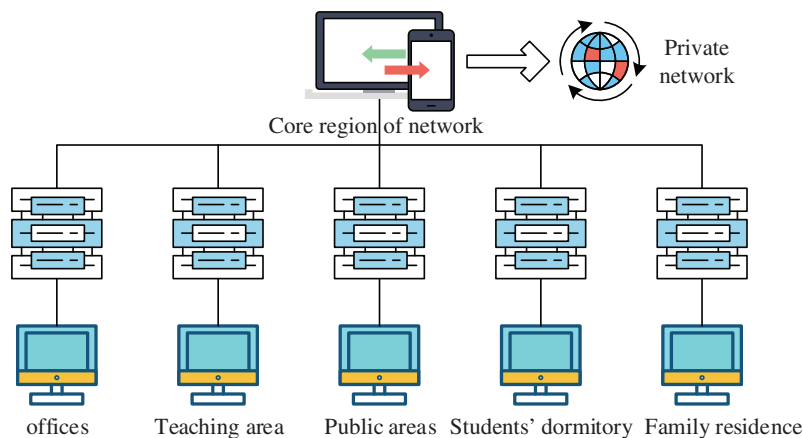
Figure 3: Environmental distribution of campus network

3.3.2 Vulnerability of Campus Network

(1) The construction of campus network covers many campuses, which brings new challenges to the network management department.

(2) The service of campus network is complex, involving many departments. With the development of campus network, more and more campus service has developed into online service, such as educational administration system, personnel system and so on.

(3) The users, who have high autonomy, are so numerous that the management mode is loose. It is impossible to enforce some security protection on computers like enterprises.

(4) The campus network lacks the same scale of financial and human support as the networks in economic, cultural and other fields.

4 Analysis of Security Issue of Campus Network

(1) Security issues of physical layer. The security problem of physical layer refers to the abnormal operation of campus network caused by improper placement of physical equipment, such as servers, routers and other network equipment or power supply equipment like optical fiber cables, suffering from natural disasters or man-made damage such as flood, fire, lightning and so on [15].

(2) Loopholes in the operating system and application software. The operating system and application software used in the campus network are various. There are inherent defects and loopholes in complex operating system and application software. The system loopholes in

Windows and UNIX has been analyzed in early research [16]. For example, typical viruses "shock wave" and "Sasser worm" [17].attack by using the loopholes of the Windows operating system. If these potential dangers cannot be found in time, they may be scanned by attackers or used in other ways, becoming the target of hackers.

(3) Intrusion of computer virus. Computer virus refers to a group of computer orders or program code that destroys computer functions or data, affecting the using of computer, and can replicate itself. It has great destructiveness, hiding in executable programs or data files, which is arduous to be detected and found by people. Once the computer virus enters the system and connects with the programs in the system, it will infect other programs and finally infect the whole computer, causing great damage to the campus network, bringing economic losses to the school, and even damage the school's reputation [18].

(4) Hacking. Once the campus network is connected to the Internet, it will face the risk of internal and external hacker attacks. The common means are network monitoring (referring to the illegal acquisition of information when transmitted between users) and session interception which refers to that the data is intercepted by criminals when transmitting, and then intercepts the information, resulting in the loss of information and the termination of the system [19].

(5) E-mail. Although E-mail is one of the earliest popular applications of the Internet, due to the defects of e-mail system itself, e-mail has become the main methods of transmission of network virus and information garbage (spam), which poses a great threat to the security of campus network. The spam about pornography, violence and reactionary content violates human morality, laws and regulations, is not conducive to the formation of students' world outlook and values [20].

(6) Other human factors. First, people's unconscious mistakes. For example, security loopholes in the system due to operational errors, or users who have weak security awareness, lend their account to others at will, which poses a threat to computer and network security. Second, the abuse of campus resources by internal users of campus network, who download free videos and software. Third, the freedom of the network. Most networks have no technical constraints of users. Users can surf the Internet freely, publishing and obtaining all kinds of information [21].

5 Preventive Strategies of Campus Network Security

5.1 Strategies for Physical Environments

The placement of network equipment are supposed to strictly comply with the provisions of national security construction, taking protective measures according to geographical characteristics, regularly checking the protection, strictly controlling the temperature and humidity of the computer room, and do a good job in security against theft and damage. Consider the distance between the wiring system and communication lines, lighting lines and heating pipes in the network. Consider the grounding safety of physical circuits in the network.

### 5.2 Establish a Centralized System of Computer Virus Prevention and Killing

With the development of computer network and the popularization of Internet application, the spread of computer virus has been separated from the standalone mode, and the standalone virus killing system has been unable to meet the killing requirements of computer virus. The campus network must adopt a centralized system of virus prevention and killing [6], establishing virus prevention and killing center in the campus network, and eliminate the virus of computers which are connected to Internet. The centralized computer virus prevention and killing system not only automatically

update the virus database, but also provide anti-virus services for extraterritorial networked computers, realizing the unified prevention and killing of computer viruses in each campus. At the same time, the e-mail virus gateway and virus engine it provides can be combined with the e-mail system, filtering virus messages.

5.3 Joint Construction of Firewall and Intrusion Detection System (IDS)

Firewall technology is one of the earliest and most widely used products to ensure network security. IDS is another line of defense appeared after firewall. The combination of them effectively ensures the safety of internal network, the developments are shown in Fig. 4.
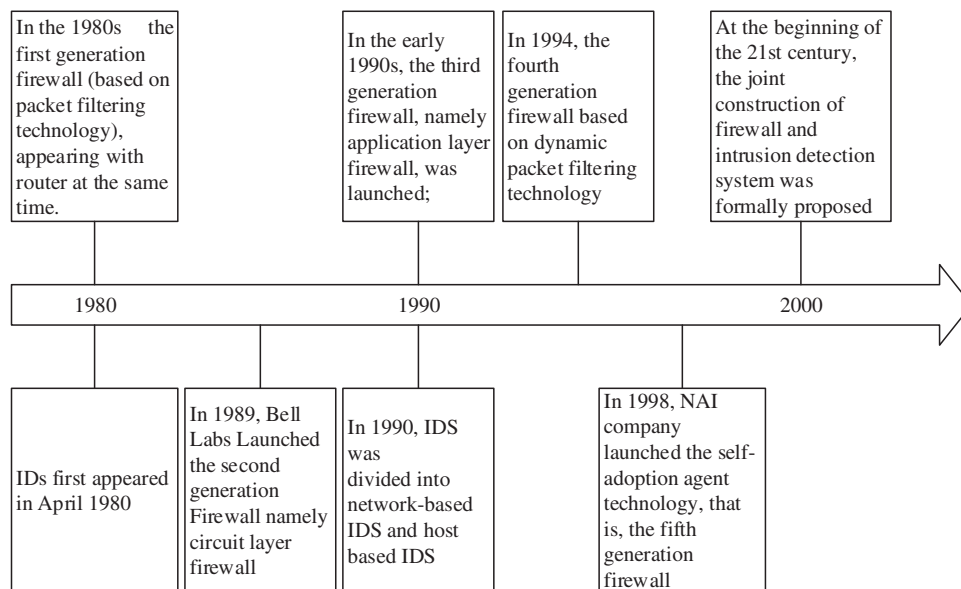
Figure 4: Developments of joint construction of firewall and IDS

Firewall [22] can be used as a blocking point of network communication. All information in and out of the network must pass through the firewall. The firewall is between the intranet and the extranet, and all transmitted information must pass through it, so the firewall is also capable in effectively recording network activities. Additionally, firewall technology provides a feasible solution to the IP address crisis.

However, with the development of virus technology and network attack technology, the firewall is no longer the "universal defense" to ensure network security. It is incapable of attacking action that bypass it, and have not the ability to prevent the virus or prevent the infected software or files from continuing to transmit. We can only install anti-virus software for the virus. Furthermore, the firewall needs a specific closed network topology to support.

The setting of firewall can be designed according to the characteristics and specific functions of campus network. At the general entrance and exit of the network, set high-performance hardware firewall; in the internal key nodes, other hardware and software firewalls are set, to flexibly set a variety of prevention strategies.

IDS [23] can monitor and analyze system events and users' behavior, testing the security status of system settings, tracking any modification to system security, and allow managers who are not in a

security fields to deal with important security events effectively. Compared with firewall system, it is more real-time. However, it lacks active defense function, but a passive and limited security defense technology. In addition to reporting, any defense measures against intrusion cannot be taken by it.

The joint construction of firewall system and IDS [24] was first proposed in the early 21st century, which can function IDS to dynamically change the defense strategy of firewall, and effectively improve the mobility and response ability of firewall. At the same time, the firewall completely cuts off the source of intrusion behavior from the source and enhances the blocking function of IDS.

5.4 Network Security Situational Awareness

The traditional network security measures concentrate on the detection and defense after intrusion, but ignore the "preventive injection" of predicting and analyzing the network security situation in advance. Network security situational awareness [5] is different from traditional network security measures. Technologies based on hierarchical analysis, machine learning, immune system and game theory are used to identify various behaviors in network activities, understanding and evaluating them on the whole, and then provide reasonable decision-making. It improves the monitoring ability and emergency response ability of the network, and helps to predict the development trend of network security in time.

5.5 Legislate and Strengthen Supervision

With the rapid development of information network and the continuous advancement of human society, network security has jumped to national security. Cyberspace, as the fifth space, is embedded in the top four major areas-"sea, land, air and space". China is supposed to actively respond to this situation, reasonably formulating and adjusting China's network security strategy, and establish and improve relevant legislation.

China has issued a number of laws related to network security, but compared with the rapid speed of the network development, the improvement of laws still lags behind, and the existing legal system is too complex, lacking of legislation on campus network security. In the future, we are also expected to concentrate on campus security legislation, setting up professional security coordination organizations, and set up corresponding organs to strengthen network security supervision, so that they could find and effectively curb online criminal activities at the first time. The campus network is also a relatively special environment, whose main users are students. Thus we ought not only to ensure the normal and safe operation of the network, but also filter out some unhealthy information that destroys social harmony and stability, providing a good legal environment for talent training [25].

5.6 Establish a Scientific Management System

The whole campus network system can be paralyzed by an unreasonable operation. Therefore, strengthening the training of network system managers, broadening the knowledge of network managers is a paramount part of campus network security construction [26]. Starting from the specific reality of colleges, we are supposed to clarify the responsibilities and powers of management staff, and the Internet facilities in all campus should comply with the principle of campus network. At the same time, we should record the operation information of managers. Once hackers are found to enter, measures should be taken in time to prevent hackers from invading, minimizing the loss of the school.

6 Conclusions

In the long run, to optimize the network environment and reduce the occurrence of network security events, in addition to technical measures, corresponding laws and regulations should also be established and improved. However, before the relatively impeccable laws and regulations appear, technical means are still a solid ensure to network security. At present, we have to start from the reality of each campus and take necessary technical measures to ensure the stable and safe operation of campus network.

Campus network security is not only a comprehensive subject, involving numerous aspects such as technology, management, and legislation and so on; but also a dynamic subject, with the development and advancement of various network technologies, new security problems will continue to emerge. Whether use various defense technologies, strengthen management or improve legislation, it is inseparable from the support of capital and human resources who mastering the latest news and technology. Therefore, colleges and universities should increase capital investment in the construction of campus network security, putting forward higher requirements for campus network managers.

A technology can only solve one problem. Only a strict and clear security reaction strategy might viably escort network security. The threats faced by campus network are diverse. After analyzing the various factors, we ought to start from the physical security construction, with the assistance of various hardware and software technologies, and then strengthen the legislation and management. Only in this way can we build a safe and viable service-oriented campus network, providing a exceptional stage for the construction of digital campus.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]   J. Q. Ju, M. Alabsi, A. A. AI-Abisi and H. Lee, "Analysis and protection of computer network security issues," in *ICACT 2020 February*, Pyeongchang, Korea, pp. 16–19, 2020.

[2]   M. Huang, W. B. Luo and X. Wan, "Assessing the security of campus network: The seven cases of seven universities," *Sensors*, vol. 21, pp. 306, 2021. https://doi.org/10.3390/s21010306.

[3]   B. Y. Zhang, "Detection and prevention of network intrusion," *Journal of Polytechnic University*, vol. 2002, no. 4, pp. 32–33, 2002.

[4]   S. S. Peng, H. M. Zhang and D. L. Bian, "Analysis of computer network security," *Modern Electronics Technique*, vol. 35, no. 4, pp. 109–113, 2012.

[5]   J. Gong, X. D. Zang, Q. Su, X. Y. Hu and J. Xu, "Survey of network security situation awareness," *Journal of Software*, vol. 28, no. 4, pp. 1010–1026, 2017.

[6]   G. T. Zha, Q. J. Peng and G. F. Luo, "Problem and policy of security system in campus network," *Application Research of Computers*, vol. 2005, no. 3, pp. 150–152, 2005.

[7]   Y. Nidup, "Awareness about the online security threat and ways to secure the youths," *Journal of Cyber Security*, vol. 3, no. 3, pp. 133–148, 2021.

[8]   M. M. Althobaiti, "Assessing user's susceptibility and awareness of cybersecurity threats," *Intelligent Automation & Soft Computing*, vol. 28, no. 1, pp. 167–177, 2021.

[9]   C. Y. Wei, Y. L. Ren and X. Lee, "Research on the construction of network security governance system in campus," *Network Security Technology & Application*, vol. 2021, no. 1, pp. 96–98, 2021.

[10]   S. A. Hassan, K. Alnowibet, P. Agrawal and A. W. Mohamed, "Managing delivery of safeguarding substances as a mitigation against outbreaks of pandemics," *Computers, Materials &Continua*, vol. 68, pp. 1161–1181, 2021.

[11]   W. Liao, "Brief analysis of short board effect in operation control," *Journal of Changsha Vocational College*, vol. 18, no. 3, pp. 72–75, 2018.

[12]   M. Wang, "Research on integrated design of campus computer network system," *Electronic Test*, vol. 2015, no. 1, pp. 129–130, 2015.

[13]   S. M. Duan, "Network design scheme of library subnet," *Journal of Modern Information*, vol. 2007, no. 3, pp. 110–111, 2007.

[14]   Y. H. Wang, "Discussion on security and optimization of campus network," *Network Security Technology & Application*, vol. 2019, no. 8, pp. 86–88, 2019.

[15]   J. M. Huang and G. G. Lee, "Research and exploration on construction management and maintenance of internet working in colleges," *Experimental Technology and Management*, vol. 29, no. 8, pp. 206–208, 2012.

[16]   Z. H. Rao and E. B. Fang, "Research plan and achievements prospects for the analysis and discovery technology of vulnerabilities in software and system," *Advanced Engineering Sciences*, vol. 50, no. 1, pp. 9–21, 2012.

[17]   Y. K. Zhang, C. G. Wang, F. W. Wang and J. F. Ma, "Analysis and prevention of sasser worm," *Computer Engineering*, vol. 2005, no. 18, pp. 65–67, 2005.

[18]   Y. Na and K. Xiao, "Research on computer virus and preventive measures," *Science &Technology Information*, vol. 2012, no. 3, pp. 129–170, 2012.

[19]   G. Q. Xie, "Brief analysis of common means and prevention of network attack," *Information Technology and Information*, vol. 2018, no. 5, pp. 129–130, 2018.

[20]   W. J. Zhang and X. A. Lee, "Study of integrated solutions to campus network security," *Electronic Technology*, vol. 2006, no. 3, pp. 64–67, 2006.

[21]   X. R. Zhang, X. Sun, X. M. Sun, W. Sun and S. K. Jha, "Robust reversible audio watermarking scheme for telemedicine and privacy protection," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3035–3050, 2022.

[22]   C. Huang, "Application of network firewall in campus network security," *Heilongjiang Science*, vol. 9, no. 1, pp. 132–133, 2018.

[23]   W. Lee and Z. M. Yang, "Review of intrusion detection system," *Journal of Jilin University*, vol. 34, no. 5, pp. 657–662, 2016.

[24]   X. D. Zhang, H. P. Hu, X. H. Kuang and H. Z. Chen, "Research and implementation of the interaction with firewalls and IDS," *Computer Engineering &Science*, vol. 2001, no. 4, pp. 22–26, 2004.

[25]   Z. G. Yu, "Embedding situation and countermeasures of network security for national security and public security," *ZGYU LegalForum*, vol. 29, no. 6, pp. 5–19, 2014.

[26]   W. Sun, G. Z. Dai, X. R. Zhang, X. Z. He and X. Chen, "TBE-net: A three-branch embedding network with part-aware ability and feature complementary learning for vehicle re-identification," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021. [Online]. Available: https://doi.org/10.1109/TITS.2021.3130403.