Journal of Artificial Intelligence Practice (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2022.050310
ISSN 2371-8412 Vol. 5 Num. 3

Computer Network Security in the Era of "Internet +"

Juan Wu[1,2,*], Dexi Chen[1,2], Haiqing Liu[3]

[1]*School of Computer and Big Data, Jining Normal University, Wulanchabu, Inner Mongolia, China*
[2]*Philippine Christian University Center for International Education, Manila, Philippine*
[3]*Jining District Experimental Middle School, Wulanchabu, Inner Mongolia, China*
1344639828@qq.com
[*]*Corresponding author*

Keywords: Internet+ Era, Computer Network, Network Security, Trojan Horse Detection

Abstract: For the majority of netizens, the Internet has opened the door to a new world for them, and obtaining information through the Internet has become a faster and more fashionable way of life. However, there are certain network security problems in many aspects, and these security problems have affected users' use of the network to a certain extent. The purpose of this paper is to study computer network security issues based on the era of "Internet +". Firstly, the definition and characteristics of Internet+ are expounded, and then some problems existing in the current Internet+ security management are analyzed. Finally, the detection technology of Internet security management and software security analysis technology are introduced in detail. It is proposed that the network security management system can solve the computer network security problems in the "Internet +" era, and it focuses on how to realize the functions of the connection of different systems, data storage, network security event monitoring and Internet application monitoring functions. The experimental results show that the system can effectively manage computer network security issues.

1. Introduction

Information technology has brought the progress of human civilization and provided convenience for human development. Internet application is an important content of information technology and plays an important role in the process of information technology [1-2]. However, it is also necessary to realize that in the context of IT, the rapid development of the Internet has also brought negative problems, one of which is network security, where cyber hacking, cybercrime, political reasons and other incidents are emerging one after another. Solving the problem of Internet + security is an important task in the information age, and it is also a problem that needs to be solved in the process of promoting the construction of informatization [3-4].

Different IPv6 transition technologies can implement communication between hosts using two incompatible Internet protocol versions in various scenarios, but they also involve additional security issues [5]. Based on the STRIDE method and its application to IPv6 transition technologies, Lencse G developed a method for identifying potential security issues of different IPv6 transition technologies and their implementations. Our approach consists of applying the STRIDE approach at two levels: the level of individual IPv6 transition technologies and their

chosen implementation level [6]. Mikryukov A A In order to improve the accuracy and timeliness of the classification of security events, security events and threats in the information security system, it is suggested to use the neural network technology as the classification tool of the information security system. These techniques allow for the inclusion of incomplete, inaccurate and unidentifiable raw data, as well as the utilization of previously accumulated information about security issues. To address this problem more efficiently, a collective approach based on collective neural ensembles with advanced complex methods is implemented [7]. Therefore, carrying out network security research under the conditions of "Internet +" can promote the smooth progress of the cause of socialism with Chinese characteristics [8].

This paper firstly studies and analyzes the security problems of computer networks in the Internet+ era, and then sorts out the entire communication technology network. Provides useful ideas for reference. These measures have been comprehensively and comprehensively considered from multiple perspectives and levels, and effectively deal with network security issues by formulating a scientific and reasonable network security management system.

2. Research on Computer Network Security in the Era of "Internet +"

2.1 Internet+

The "+" mentioned in "Internet +" is not a physical reaction produced by mechanically sticking the Internet and traditional industries together, but a chemical reaction of deep integration of the Internet and traditional industries to transform traditional industries [9-10]. "Internet +" is the embodiment of the national will and the will of the whole people. It will not be a literal concept. From reporting to planning, from strategy to action, it will have a very long-term and profound impact on the economy and society in the future., and will definitely converge into a powerful force to promote the advent of a new era [11-12].

2.2 Several Problems Existing in the Current Internet + Security Management

(1) The legal environment is relatively poor

At present, many administrative regulations and departmental regulations that have been formulated have many vague areas in terms of content, which are relatively general, and become helpless when solving complex practical problems [13-14]. In addition, many clauses were formulated without comprehensive consideration of possible changes in the actual situation, and they did not do enough to predict changes. As a result, not long after the legal norms were introduced, the security issues on the Internet had changed a lot, and the promulgated regulations could not solve practical problems at all, and sometimes even hinder the solution of the problem. At present, although there are many administrative regulations and departmental regulations in the field of Internet supervision, many regulations are actually a waste of administrative resources and are on the shelf. Seriousness and authority are called into question. There is a serious lack of supporting legal system for administrative law enforcement, which makes it difficult for existing laws and regulations to meet the needs of the rapid development of the Internet business. Many emerging problems cannot be effectively solved through laws, and many blank spots in the legal system have appeared [15-16].

(2) Lack of safety management

At present, the government's management of Internet security, especially the security risk management of e-commerce and online banking, is not enough, and the management capacity needs to be improved. Although there are many management departments, each department is basically "cleaning the snow before the door". There is no unified and efficient security management

network, and many Internet supervision departments are still relatively backward in technology and equipment, and their technical capabilities are relatively poor. When dealing with rapidly changing Internet security supervision issues, they appear to be lagging behind [17-18].

2.3 Internet Security Management Detection Technology

A Trojan is a specific program used to control another computer. Trojans usually have two operating systems: one is the server (control side), and the other is the client (control side). It is a server that is implanted on an infected computer, and clients try to connect to the server. After the connection is established, the Trojan starts running. Once the Trojan is running and connecting from the control group, the control group will have the same permissions for operations as the server group, such as changing the computer configuration, adding a password to the computer, performing any operations on files, changing the registry, and more.

Real-time search technology mainly monitors various machine operations in real time, such as file creation, process creation, etc. Feature library is also an important part of this type of detection technology. Through data mining technology, unknown viruses or viruses that are not completely detected and killed in massive data can be detected.

3. Investigation and Research on Computer Network Security Issues in the Era of "Internet +"

3.1 Network Security Management System

The information security management subsystem is an information security management system with functions such as basic data management, access log management, and information security management. The information security management subsystem (NMMS) is linked with the operator's information security management system (ISMS) through the information security management interface to realize functions such as basic data management, access log management, and monitoring and disposal of illegal websites.

3.2 Naive Bayes Classifier for Trojan Horse Detection

The principle of the simple Bayesian classifier is to use the known prior probability of an object to calculate the probability of each class, that is, the posterior probability, and use the Bayesian formula to select the class with the highest probability as the object category. For Trojan horse detection, the program is divided into two categories: Trojan horse program and legitimate program (set Trojan horse as s1, legitimate program as s2,), S={s1, S2}. There is another unknown program X, and its behavioral characteristics are X=(x1, X2,..., Xn}, then the Bayesian classifier is applied to obtain the category S of the program X and denoted as Sx, then there is the following formula:

$$s_x = \arg\max_{i=1,2}\{P(S = Si \mid X = x)\} \tag{1}$$

Naive Bayes requires attributes to be independent of each other, that is:

$$P(x_i, x_j) = P(x_i)P(x_j), (i, j = 1,2,...n, and \quad i \neq j) \tag{2}$$

Assuming that there are m Trojan horses and n normal programs in the sample training set, we can get:

$$P(S_1)=\frac{m}{m+n};P(S_2)=\frac{n}{m+n} \quad (3)$$

According to the above formula, the probability of program X in two categories can be obtained, and X is classified as a category with high probability. This is the process of using the naive Bayes classifier to determine the Trojan program.

4. Analysis and Research on Computer Network Security Issues in the Era of "Internet +"

4.1 Basic Data Management

Basic data management includes basic data query and abnormal monitoring of basic data. As shown in Figure 1:

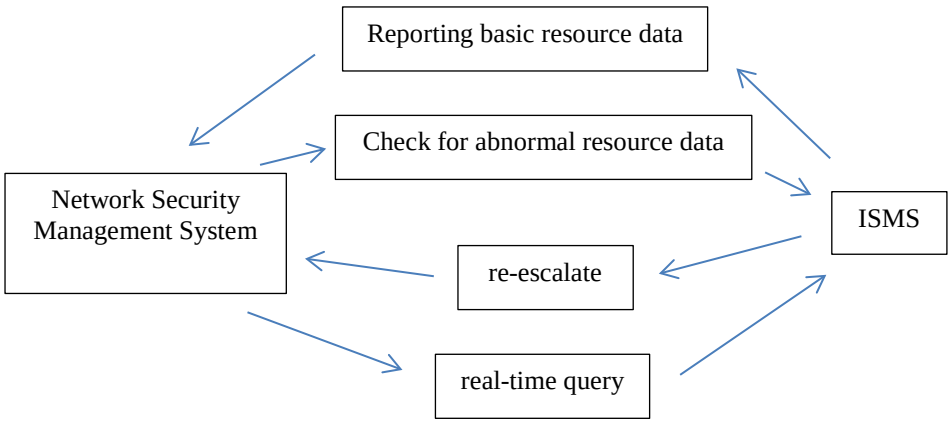

Figure 1: Basic resource management

The core data records include IDC/ISP division, IDC/ISP customer-related information files, and resource information files related to all IDC computer industry fields/ISP divisions under the IDC/ISP trade group. The information security management system authorizes master data requests to the operator's information security system (ISMS) through the ISMI interface, performs master data request and request functions, and tracks external records.

NMMS can request ISMS core data files and foreign tracking files, logs, active resource tracking files, illegal website tracking files, illegal information tracking and rejection files, etc. in request order. Standards-compliant data records are asynchronously reported to NMMS through the data reporting process. The NMMS feeds back the verification result of the main data file reported by the ISMS according to the request command flow. The request command processing flow is as follows:

(1) The NMMS system calls the idc_command() method to issue a request command to the ISMS. The description is embedded in the XML file format.

(2) The ISMS receives the authorization request issued by the SMS and verifies the authorization in detail. After the verification is completed, the request order is saved, and the status of the order received by the same connection is reported in time. If the ISMS does not successfully receive the given order, the SMS must be resent.

(3) The query result statement returns the query result by calling the data reference process.

4.2 Network Security Incident Monitoring

Network security incidents: including WEB attack incidents, network attack incidents, Trojan horse virus incidents, DDOS attack incidents, and WAF incidents.

Data content: attack time, source IP, source area, destination IP, destination URL, destination area, destination port, protocol, event category.

Display method: switch according to the dimension of the world map; quasi-real-time display of network security attack events discovered in the previous monitoring cycle, dynamic display of attack behavior from the attack source to the target, and different colors to indicate the number of attack events. TOP10 display (attack source, attack target, event category table) displays the TOP10 attack events in the previous monitoring period, which can be sorted by source IP, target IP, event type, source area, and target area.

According to the monitored network security data of the whole province, conduct statistical analysis on the resource monitoring results of important user networks, including statistics on website security vulnerabilities, equipment monitoring, and website service monitoring, and provide rich statistical reports, as shown in Table 1. The monitoring task statistics are shown in Figure 2.

Table 1: Statistics

City name	Number of vulnerabilities	The number of website hanging horses	Number of phishing sites	Zombie Controlled IP Number
M city	25	6	1	1
City B	18	2	2	1
L city	31	9	3	2

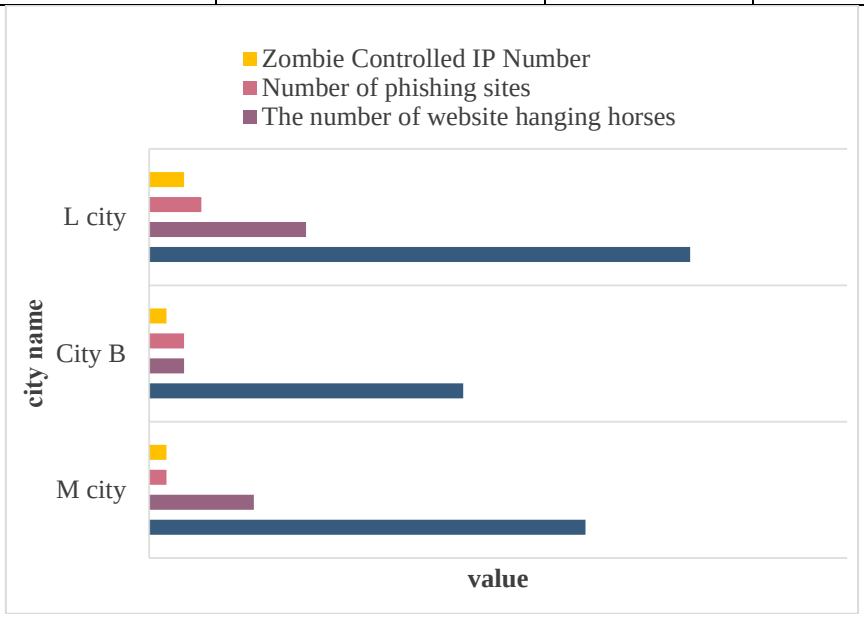

Figure 2: Monitoring task statistics

5. Conclusions

In the information age, the Internet has become an important part of people's work, life and study. At the same time, cybersecurity issues such as cybercrime, cyberbullying, and hacker attacks continue to emerge. These not only affect the social and economic life of ordinary people, but also affect national security. Therefore, in the field of Internet +, security is an increasingly important issue, and it is also a difficult problem that needs to be overcome urgently. This paper

systematically studies the network security issues under the "Internet+" condition, and discusses the related concepts of network security under the "Internet+" condition, the detection technology of Internet security management, the practical challenges faced by the Internet+ security management, and the maintenance of network security. Valid path. However, the knowledge reserve for interdisciplinary fields is still insufficient in this study. From the research conclusion, the conclusion of this research is mainly on the countermeasure analysis of the network security work in the strategic deployment, and lacks the theoretical research and practical exploration of the specific implementation mechanism.

References

[1] Raj N M, Midhunchakkaravarthy D, Bhattacharyya D. Security Issues and Various Attacks in Wireless Sensor Network: A Survey [J]. International Journal of Security and its Applications, 2019, 13(3):9-16.

[2] Shyamala R, Prabakaran D. A survey on security issues and solutions in virtual private network [J]. International Journal of Pure and Applied Mathematics, 2018, 119(14):1183-1191.

[3] Gowthami K. Security Issues on IoT Environment in Wireless Network Communications [J]. International Journal of Wireless Networks and Broadband Technologies, 2019, 8(2):31-46.

[4] Chriki A, Touati H, Snoussi H, et al. FANET: Communication, mobility models and security issues [J]. Computer networks, 2019, 163(Nov.9):106877.1-106877.17.

[5] Anand A, Trivedi N K, Kumar A. Data Security Issues and Their Solutions in Cloud Computing [J]. Journal of Critical Reviews, 2020, 7(14):2597-2604.

[6] Lencse G, Kadobayashi Y. Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64 [J]. Computers & Security, 2018, 77(AUG.):397-411.

[7] Mikryukov A A, Babash A V, Sizov V A. Classifcation of events in information security systems based on neural networks [J]. Open Education, 2019, 23(1):57-63.

[8] Olimid R F, Nencioni G. 5G Network Slicing: A Security Overview [J]. IEEE Access, 2020, PP (99):1-1.

[9] Ichaba M. Security Threats and Solutions in Mobile Ad Hoc Networks; A Review [J]. Universal Journal of Communications and Network, 2019, 6(2):7-17.

[10] Chatterjee T, Ruj S, Bit S D. Security Issues in Named Data Networks [J]. Computer, 2018, 51(1):66-75.

[11] Alenezi M, Almustafa K, Hussein M. On Virtualization and Security-Awareness Performance Analysis in 5G Cellular Networks [J]. JOURNAL OF Engineering Science and Technology Review, 2018, 11(1):199-207.

[12] Dunn K. WatchGuard Technologies Firebox M270 w/Total Security Suite [J]. Sc Magazine, 2019, 30(3):40-40.

[13] Venkata K, Srihari, Karthik. A survey on certain investigation on security issue of the security model in hybrid cloud [J]. International Journal of Pure & Applied Mathematics, 2018, 118(9):113-122.

[14] Kumar S, Singh K, Kumar S, et al. Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning based Security Approach [J]. IEEE Access, 2019, PP (99):1-1.

[15] Bagaa M, Taleb T, Bernabe J B, et al. QoS and Resource-aware Security Orchestration and Life Cycle Management[J]. IEEE Transactions on Mobile Computing, 2020, PP (99):1-1.

[16] Ali M, Malik S, Khalid Z, et al. Security Issues, Threats and Respective Mitigation In Cloud Computing -A Systematic Review [J]. International Journal of Scientific & Technology Research, 2020, 9(8):474-484.

[17] Vk K. A Novel SDN Architecture for IoT Security [J]. Journal of Scientific Research and Development, 2020, 4(2):48-52.

[18] Perminov P, Kosachenko T, Konev A, et al. Automation of information security audit in the Information System on the example of a standard "CIS Palo Alto 8 Firewall Benchmark"[J]. International Journal of Advanced Trends in Computer Science and Engineering, 2020, 9(2):2085-2088.