Research on Information Security Risk Assessment Strategy on China's Campus Based on AHP Method

He Honglin

Assets and equipment management department of Pingxiang University, Pingxiang, 337055, China

Keywords: Campus Network; Information Security; Risk Assessment Strategy; Analytic Hierarchy Process

Abstract: With the development of university's networking, the campus network infrastructure capital construction in universities is completed. The school is employing and disposing them such as scientific research, teaching, network working and online amusement to the applications of campus network. In the initial stage of networking, there is little construction in such aspects as safe consciousness and safety management but primarily in the usability. Especially in some technical colleges, it is nearly a blank in safety constructions. This leads the network incidents to happen constantly, so the security of campus network is facing a great threat. With the development of campus network informatization, how to build up a reliable campus network security protection system is an issues that cannot be ignored. The research of this subject is to consult relevant materials to obtain the theory knowledge about the campus online security, summarize gains and experience over the past six years work in campus network and management. The strategy can also be used in technology and other network environments of employing the background to similar to campus network, the originally safe tactics have passed operation and test of the real network environment of researcher's unit of this subject finally.

1. Introduction

As a campus information infrastructure, campus network is an important platform for schools to realize informationization [1]. In the teaching, research, management and foreign exchange window and many other important platforms play a decisive role. With the continuous expansion and upgrading of campus network, the network scale becomes larger and larger, the difficulty of network management is also increasing day by day, the potential safety hazard in campus network accumulates continuously too [2]. While the Internet brings convenience to us, various network security vulnerabilities are constantly being discovered and exploited due to the openness, interconnectivity and sharing characteristics of the network [3]. Viruses, Trojans, hackers, unhealthy information and so on, all the time threatening the healthy development of the campus network, education has become an inevitable issue of information technology [4]. In recent years, a problem that should be paid more attention to by college network managers is that the computer-related technical level of network users in vocational colleges is very high, some completely exceeding the imagination of managers. According to statistics, 80% of attacks on campus networks come from the campus network, due to campus staff inside the campus network data loss, college service is attacked to modify, the network paralysis occasionally happen, and now the campus network is in the dual network of internal and external factors work under stress [5]. According to the current network situation, how to build an efficient, safe and stable campus network environment is a must for all colleges and universities [6].

To build an efficient, safe and stable campus network, the general practice of colleges and universities is to invite all kinds of integrators who usually have business with their own schools to design web-based applications for schools and give an initial security solution [7]. Network managers to modify and improve. However, often due to limited funds, schools are prone to input costs are mainly used in network infrastructure above, network security investment in the construction is quite limited. And most of the solutions proposed by the integrators are often used to solve the specific technical problems related to security solutions, it is not very suitable for the overall construction of the school network security. How to build a campus network overall security solutions. The topic of this paper is just put forward in this context - based on analytic hierarchy process of campus network security policy research and implementation.

2. Common Cybersecurity Issues

Computer virus in the "People's Republic of China Computer Information System Security Regulations" is defined as: "Computer virus refers to the establishment or insertion in the computer program to destroy computer functions or data, affect the computer and can copy a set of computer instructions or code ". From a development perspective, a computer virus is a type of malicious code that is deliberately written as a collection of destructive computer programs or instructions. Due to several characteristics of viruses, such as self-replication, invisibility, latentness and unpredictability, most attackers attacked attackers by creating viruses or Trojans, resulting in wasted resources, system damage, data loss and other issues. After the rapid development of the Internet in recent years, the phenomenon that viruses and Trojans are used in cybercrime is gradually increasing. There are more and more viruses and Trojans for illegally obtaining accounts and passwords with real economic significance such as banking, securities, e-commerce, QQ, online games and so on.

According to "2016 China Computer Virus Outbreak and Internet Security Report" pointed out: In 2016, China trojans have seen an explosion in the number of new computer viruses and viruses in the country. Trojans still exist in the virus while retaining its original features. As shown in Figure 1, the Internet has become modular in modularity, specialization, and virus "operations".

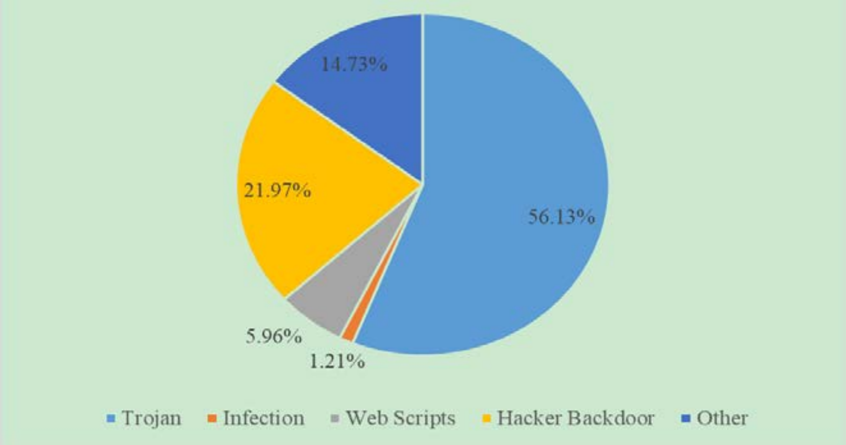

Fig.1 Different types of virus infection ratio

2.1 Network Protocol Vulnerability

TCP / IP protocol cluster is currently the most widely used Internet protocol stack. Since the original protocol was proposed for use as an Internet-based protocol, there are many security vulnerabilities in the security design mainly due to its ease of use and high efficiency.

TCP protocol: A normal TCP connection completes the communication through the "three-way handshake". Potential security may exist in various attacks such as TCP / IP sequence number attacks, TCP / IP session hijacking and TCP SYN attacks.

UDP protocol: As the protocol does not control the message, only consider how to quickly and easily transfer data, all security is lower;

ICMP protocol: According to RFC791, the maximum length of IP packet is up to 65535 octets. Packets larger than the maximum transmission unit (MTU) length must be fragmented and reassembled during transmission. There is fragmentation fragmentation in the process of fragmentation: overlapping fragmentation reorganization loopholes, changes in offset variables;

DNS protocol: The source and destination ports of the protocol communication are UDP53, so malicious users can attack the client and server by monitoring the normal DNS communication and forging the non-existent record.

SMTP protocol: In addition to using special programs such as PGP and S / MIME, most email programs lack authentication, confidentiality and can be attacked by e-mail bomb and spam.

ARP protocol: The ARP protocol is a running mechanism for mutual trust between hosts. The main security issues are: the host address mapping table is dynamically tampered with; the ARP request is disguised as ARP reply packet;

RPC services: RPC programs are often attacked by buffer overflows when executing distributed applications, because they do not perform a full error checking or enter a validity service.

2.2 Operating System Security

The operating system is a collection of all the hardware, software, and data resources that govern the computer system. In 1985, the United States Department of Defense put forward TCSEC (Orange Book), a trusted computer system evaluation standard. The Orange Book defines a rigorous and complete evaluation of the operating system. However, current operating systems have strong security features: support for user authentication, management, auditing, etc. However, Jeff Jones, chief strategy officer of Microsoft's security technology department, reported the vulnerability statistics of client operating system in the first quarter of 2008, Table 1 depicts a comparison of vulnerabilities in seven different operating system client operating systems. Figure 2 depicts a comparison of vulnerabilities discovered by each operating system. From these two figures, it can be seen that there are still many potential threats to today's popular operating system. All current operating systems are still far less than the requirements of TCSEC.

Tab.1 Seven Client Operating System Vulnerability Comparison

Client OS	Vulnerabilities	Security Advisories	Patch events
Windows Vista	Vista	9	6
Windows XP	12	8	2
Red Hat RHELD 5 (reduced)	60	19	12
Red Hat RHELWS 4 (reduced)	75	18	14
Ubuntu 606 (reduced)	LTS	54	15
Mac OS X 10.5	Leopard	83	6
Mac OS X 10.4	Tiger	81	5

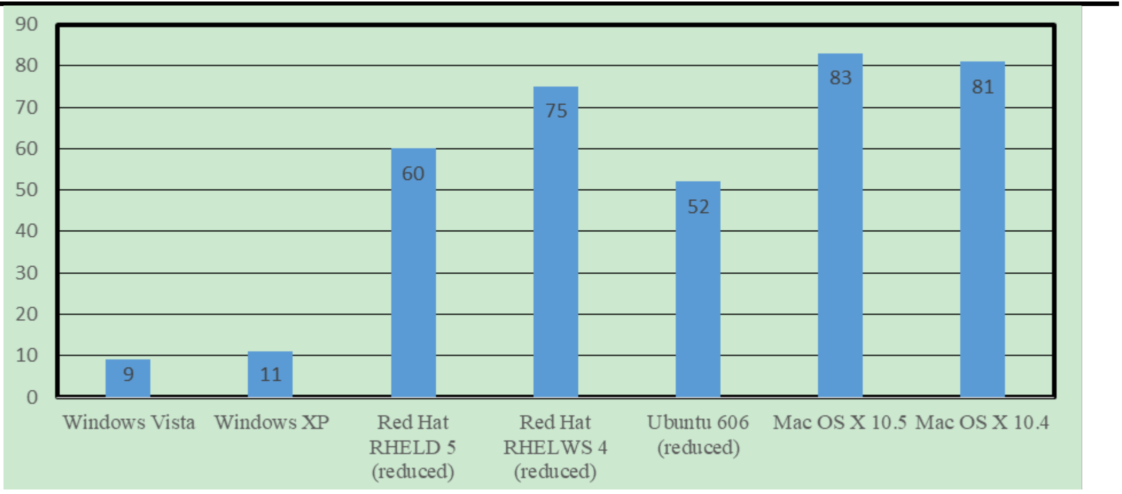

Fig.2 High-risk vulnerability comparison

3. Risk Assessment

Sean Convery explains three major steps in developing a security system in Network Security Architectures: testing security policy drivers and designing security systems. There are two main drivers of testing security policy drivers: business requirements and risk analysis. Risk assessment refers to the positioning of network resources and a clear attack can occur energetic, including clarifying key assets, valuing assets and determining the likelihood of damage. Cyber risks consist mainly of assets, vulnerabilities and threats. Before making a risk assessment, identify the assets that need protection. Table 2 lists some of the network assets that may need to be considered.

3.1 Threats and Vulnerabilities

Once you have identified your network assets, you should identify potential threats to your assets and the possibility of assets being attacked by this threat. Threats can be any person, object or incident that may cause damage to the network or network equipment. Threats can be malicious or incidental, with the result that the data may be modified, the files deleted, and so on. Vulnerability is a flaw in the network that can be exploited. Such as the user's weak password settings, it may lead to an intruder in the guess password after the unauthorized access to the network, resulting in a network threat.

Table 3 lists typical cyber security threats. Among them, the campus network threats and vulnerabilities mainly in the following forms: physical security of network resources; network eavesdropping and network information is stolen; network resources are not accessible; unauthorized access to network resources; network data is illegally manipulated.

Tab.2 Campus Network Assets

NO.	Asset	Description
1	Hardware	workstations, personal computers, printers, routers, switches, firewalls, application servers, etc.
2	Software	operating system, application, communication program, source code
3	Data	online save and offline archive data, backup, audit log, database, communication media to transmit data
4	Staff	students, teachers, administrators, management, network administrators
5	Network Performance	network bandwidth, speed

Tab.3 Typical Cyber Security Threat

Threats	Description
Eavesdropping	Sensitive information transmitted over the network is tapped
Retransmit	An attacker got some or all of the information in advance, and later sent this information to the recipient
Counterfeit	attackers send fake information to recipients
Tamper	attacker to legitimate users of the communication between the information to modify, delete, insert, and then sent to the recipient
Unauthorized access	Access to the system through counterfeit, identity attacks, system vulnerabilities and other means, so that illegal users into the network system to read, delete, modify, insert information and so on
Denial of service attacks	Attackers slow down or even paralyze system responses in some way, preventing legitimate users from gaining access to services

3.2 Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) is a method to make decisions on some complex and obscure questions, and is often used in those problems that are difficult to be completely quantitatively analyzed. It is a simple, flexible and practical multi-criteria decision-making method proposed by Professor T. L. Saaty in the early 1970s. The principle of AHP is to first define the problem to be solved by a complex system of many factors that are interrelated and mutually constrained. Then the problem is organized and stratified, and then a mathematical model is used to construct a structured model. The factors are hierarchically sorted to assist in decision-making.

The hierarchical order and consistency test can be described as follows: judging that the matrix $\boldsymbol{A}$ corresponds to the eigenvector $\boldsymbol{W}$ of the largest eigenvalue $\lambda_{\max}$, the normalized weight is the ranking weight of the corresponding factor of the same level to the relative importance of the factor of the previous level. This process is called hierarchical single rank. Although the method of constructing the judgment matrix can reduce the interference of other factors, it relatively objectively reflects the difference of the influence of a pair of factors. However, when all the results are compared together, they may include some degree of non-uniformity.

3.3 Campus Network Risk Analysis

Threats and vulnerabilities in campus networks are a major risk factor, so factors for risk analysis can be defined: physical security, network availability, unauthorized access to information, manipulation of data, and theft of information. According to AHP method, Table 4 lists the risk analysis results of five risk factors of campus network:

Tab.4 Campus Network Risk Analysis

Risk Factors	B_1	B_2	B_3	B_4	B_5	Risk Impact	Risk Probability	Risk Level
	0.0379	0.4197	0.2054	0.0744	0.2626			
Physical security	0.1	0.1	0.1	0.1	0.1	0.1	1	0.1
Network availability	0.6	0.7	0.7	0.5	0.7	0.681	3	2.043
Information is not authorized to access	0.7	0.7	0.5	0.6	0.7	0.672	9	6.048
Data manipulation	0.7	0.6	0.6	0.7	0.6	0.611	4	2.445
Information stolen	0.3	0.1	0.3	0.1	0.1	0.149	20	2.973

As a result, it can quantitatively analyze the rankings of the campus network by different risk categories: unauthorized access to information (6.048), theft of information (2.973), data manipulation (2.445), network availability (2.044) and physical security (0.1), then according to the destructive risk to develop different security strategies to prevent.

4. Conclusions

Based on the network security triad, the subject carefully analyzes the campus network architecture. According to the theory of fuzzy mathematics, this paper establishes a network risk analysis model based on AHP, and applies the model to effectively analyze the campus network risk. According to the analysis results, the current variety of network security technology to develop campus network security strategy.

Cyber risks consist of assets, vulnerabilities and threats. Cybersecurity policies define the framework for protecting assets. For the development of a network security strategy, to understand and be able to meet the needs of network users is the most basic and effective risk analysis of assets is the most critical risk assessment results based on the establishment of security strategy is the most important, through the network Technology and non-technical and other ways to achieve security in the campus network strategy is the ultimate goal.

The core research content of this subject is risk analysis, which is the theoretical basis of this research. Only by correctly and accurately evaluating the existing network risks can we ensure the effectiveness of strategy formulation. The subject studies the method of AHP based on quantitative analysis of network risk, thus avoiding the ambiguity of qualitative analysis.

References

[1] Taylan O, Bafail A O, Abdulaal R M S, et al. Construction projects selection and risk assessment by fuzzy AHP and fuzzy TOPSIS methodologies[J]. Applied Soft Computing, 2014, 17: 105-116.

[2] Samvedi A, Jain V, Chan F T S, et al. Information system selection for a supply chain based on

current trends: the BRIGS approach [J]. Neural Computing and Applications, 2016: 1-15.

[3] Venkatesh V G, Rathi S, Patwa S. Analysis on supply chain risks in Indian apparel retail chains and proposal of risk prioritization model using Interpretive structural modeling[J]. Journal of Retailing and Consumer Services, 2015, 26: 153-167.

[4] Teng F W. Analysis of the Supply of and Demand for Financial Certificates in the Taiwanese Banking Industry: An Approach Using the Fuzzy ANP Model [J]. 2015.

[5] DENG L, LIU B. The Establishment and Evaluation of the Campus Network Security System Quantification and Index System Based on ABC Screening Method[C]//Computer Science and Technology: Proceedings of the International Conference (CST2016). 2017: 272-277.

[6] Rajaeian M M, Cater-Steel A, Lane M. A systematic literature review and critical assessment of model-driven decision support for IT outsourcing [J]. Decision Support Systems, 2017, 102: 42-56.

[7] Han L I, Jia Y A O. An Evaluation Research of Laboratory Safety Management Based on the Model of Matter Element and Entropy Weight [J]. Research and Exploration in Laboratory, 2015, 2: 076.