Computer Network Security: A Survey

Anita Handa

*Department Of Computer Science, Dronacharya Institute of
Management & Technology Kurukshetra, India
E-mail: anitahanda29@gmail.com*

Abstract—*Analysis of computer network security is done to integrate resources related to computer network technology and resources related to security system to build a computer network security model. This article start with the current situation of security of computer network and analyze the influential elements of computer network security and security property of computer network to provide references for security property of computer network model.*

Keywords: *computer network security; security factors; security property.*

1. INTRODUCTION

With the development of technology, computer technology has grown to maturity and become the hard core of world's development. We all use computer technology in our day to day life, for example network communication, office software etc. With the help of the internet and computers computer technology work and entertain people up to the level of their satisfaction. When used for a long time, there would be some security problems in computer network communication. Since computer network technology has spread into our life and work, these problems would badly effects the security of data and other personal information related to usage of network communication. To tackle these usually occurred problems, we need to establish a security analysis model based on the researches of computer network security to make sure computer network can work safely. With the development of computer technology, internet security analysis model has already exists. But the astonishing of speed of the development of technology greatly reduced the effect of current computer network security as an analysis model. As a result, computer network security problems occurred frequently these years. In terms of current scenarios, it is very urgent to build a complete computer network security analyzing model.

2. CURRENT SITUATION OF COMPUTER NETWORK SECURITY

2.1 The idea of security of computer network

The computer network security we talk about actually is the security of computer network, security of important data in the network system and the structural completion of computer network. To accomplish computer network security is to protect users' data and computer system from malicious attacks and steals from outside. People who work on protection of computer network security are technical material analysis engineer of computer network security. They protect the network system from computer security problems that would influence the security of users' computers, like steal, collapse, interrupt etc.

2.2 Current developmental situation of computer network security

Nowadays, computers are popularized and became an indispensable part in people's life. People use computer network communication technology to communicate with friends, finish works, learn new knowledge and entertain themselves. The development of computer technology is changing people's way of living and improving the quality of life. However, computer network security still bothers people. It is a serious problem to the world. There are a lot of computer network security specialists working on in-depths researches in computer network security. They have set up special researches on the maintaining, destruction and repairing of computer network security. Based on these research results, specialists built the PPDRR computer network security model. Through the PPDRR computer network security model, people can accomplish monitoring and analyzing computer network security. Through the PPDRR computer network security model, specialist can detect the vulnerabilities of computer network system and react in time to protect computer network system from leak of information and economical loss.

The designing of computer network security involves a wide range of specialties. Any professional knowledge related to computer could be involved, for example software design of computer software development, monitoring and maintenance of software could all use the protection of computer network security. The protection of computer network security could protect developed technology and avoid economic loss. Therefore many computer network security specialists work on the design, protection and research of computer network security, hoping to find an effective method of computer network security or a way to investigate the attacker of

computer network system. Through large amount of researches, specialists proposed a new analysis method of computer network security-- "attack-tree". Specialists integrate past attacking data and use mathematical formulas to represent them. This kind of method is called "attack-tree". Although this method still have some flaws and disagreements in integrating and explaining the "leaves". Therefore some specialists also proposed "privilege graph" analysis method to improve past computer network security analysis methods. Specialists proposed to improve old analysis method to develop new computer network security analysis methods. With the development of technology, there have been continuous innovations of computer network security analysis methods. And model building of computer network security has matured continuously. Although there has not been a specific analysis method and model that could solve all of computer network security problems. But the way of scientific is being continued. Computer network security model building is still being worked on.

3. INFLUENTIAL ELEMENTS OF SECURITY OF COMPUTER NETWORK

3.1 Attack of hackers

Hacker refers to people with great computer network skills but use them to sabotage the internet or steal information. Currently, hackers are the number 1 influential element of computer network security. The main operational principle of hackers' attack on computer network security is to use their great skills of computer network to enter the system to collect data. Then they use collated data to monitor every computer in the network system to find the vulnerability of the network to sabotage the system and destroy computer network security system. Most hacked use Trojan horses and worm virus to attack users' computers. Some hackers with great knowledge base would also write large amount of false programs to install on users' computers to control their computers. Some hackers would also monitor user's internet data to steal users' accoun t numbers, passwords and bank savings. Users would have great loss. In order to protect users' personal information and avoid malicious consequences, we need to set up a computer network security model to monitor internet security. There would be threats like communication threat, application treat and system threat in hackers' attack. Communication attack refers to the situation that users' information in communication is required by a third party. Application threat refers to that in the working process of computer network, because of programs leaks users' information is leaked to hackers and creates loss. System threat refers to the threat where system vulnerability resulted in hacker attack.

3.2 Software system and vulnerability of network system

In computer network security, vulnerability of network and software is the second influential element of computer network security after hacker attack. Vulnerability of computer network and software includes vulnerability in computer system and software design, lack of protection of computer network and software security, illegal users enter users' computer through computer network vulnerability and computer being controlled maliciously by unknown users. This high-risk vulnerability could severely influence user's daily use of computer and normal network communication. It would cause users' information cannot spread and receive. With this high-risk vulnerability, computers could be attacked; information could be steeled any time by any unknown people. It would directly influence the security of computer network system and cause great loss.

3.3 Falsification of users' personal information and leak of classified information

Falsification of users' personal information and leak of classified information is the third element of computer security. In the whole process of computer network communication, information got spread the most is personal information of users and classified materials. Therefore, we must pay special attention to the protection of users' personal information and classified materials. Falsification of users' personal information refers to the action that with the transfer of users' information, a third party intercept, falsify and delete the information to result in the interception and steal of users' information. Leak of users' information refers to unknown personnel monitor users' computers remotely and steal information through computer network. Illegal transfer of users' information refers to the illegal steal or borrowing of information without the acknowledgment and permission of user meanwhile create loss. Nowadays' society is a society of technology development. The universal use of computer technology has a great influence on people's life. Computer network technology has influences on people's life, economy and politics. But this kind of influences is two-sided. There are good influences and bad influences. Computer network technology brings people's life convenience and threat to the security of personal information. This vulnerability of computer network security brings a lot problem and causes the users of computer network great loss.

4. NATURE OF SECURITY OF COMPUTER NETWORK

Security assessment of computer network security is based on the analysis of users' computer network system. Main functions are monitoring whether there are mutations in computer network system and software. It requires a convenient, flexible and complete model to process the analyzation to avoid the complexity of space system.

4.1 Need of security of computer network

The need of security of computer network is to fulfill users' requirements of computer network's integrity and confidentiality during the usage of computer network. Through a complete systematical security strategy, computer

security is insured. The strategy of security of computer network's usage can help computer system to judge users' process of usage to prevent unknown attack. It can also insure the system's main movements could reach the requirements of computer network security. With different computer usage, the need of computer security nature could be divided into different risk level based on the use, in order to protect the security of computer network and analyze specific security feature based on specific requirements. In practical use, computer confidentiality risk levels are shown in table 1.

Table 1: Confidential risk rating scale

Classification	Feature description
C1	Show host availability
C2	Gets a OS type and version number
C3	Gets the application and version information
C4	Existence of detecting objects in the target host.
C5	Read some user specific information
C6	Read more ordinary user files
C7	Read a certain privileged documents or kernel system processes spatial content
C8	Read arbitrary files or system privilege configuration file content monitoring network activity

From the table, we can see that every level are rather separated but also connected to each other. Every level could be regarded as a kind of users' requirements of computer security. This is the separated part. They do not conflict each other. When unknown personnel attack the computer, after the security feature is destroyed, other risks would appear. Different levels of security vulnerability would influence the occurrence of risks. That's where they are connected.

4.2 Threats the security requirements are facing

Different professions have different requirements of the security of computer network system. The protection ranges are also different. Specialists put the relationship between security requirements and different threats into table 2.

Table 2: Safety requirements and threats

Threat	Safety requirement								
	Confidentiality	Integrity	Audit	Usability	Reliability	Connectivity	Recovery	Non repudiation	Uncertainty
System threat	x	x	x	x	x		x	x	x
Communication threats	x	x	x	x	x	x			
Physical threat	x						x		
Personnel threat	x				x		x		
Operation of environmental threats	x								
Application of threat	x	x	x	x	x		x	x	x
The performance of the threat				x	x	x			
The design correctness threat	x			x	x	x			

Through table 2 we can see that system threat, communication threat and application threat are the most influential factors of users' security of computer network. System threat appears when computer network system itself has vulnerability like Trojan horse, backdoor programs and system leak. Communication threat would appear when computer network communication is monitored and intercepted. Application threat would occur when system's programs create problems like IIS, FTP. Therefore, analyze an effective way of attack and attack result are the main elements of improving computer network security.

4.3 Access permission

In the actual use of computer network, system could be set to give different users' different levels of access. Foreign counties have analyzed this kind of usage carefully and designed table 3 to limit different users' access of the system.

Table 3: Access level

Access authority	Role description
Root	The system administrator, equipment management system
Superuser	The user has some special permissions are not ordinary users
User	Any of a system of ordinary users, with independent private capital resources
Guest	Anonymous login to access the computer system of the guests
Access	Remote visitors can access network services, usually trust visitors, can scan the system information

5. CONCLUSION

With the development of computer network technology, computer network security problems happen all the time. Therefore, people hold worries towards the development of computer network technology. Since computer network security influences people's life, researches to build a computer network security model must be continued.

REFERENCES

[1] Huang Zhilong. Research on computer network security analysis model [J]. *Research on computer network security analysis models***2014**(05).

[2] Zhang Tao; Hu Mingzeng; Yun Xiaochun, Zhang Yongzheng. Research on computer network security analysis model [J]. *Journal of communications*, **2005**(12).

[3] Zhang Baoshi. Research on computer network security analysis model [J]. *Electronic technology and software engineering,* **2014**(04).

[4] Hong Yaling. On modeling of computer network security [J]. *Computer CD Software and Applications*, **2013**(02).

[5] Xv Liuwei. Modeling of computer network security [J]. *Computer CD Software and Applications*, **2013**(06).