Computer Network Security Threats and Treatment Measures Based on Host Security Protection

Jianfeng Jiang1,*
1Suzhou Industrial Park Institute of Services Outsourcing, China, 215123
*Corresponding author e-mail: jiangjf@viso.edu.cn

Abstract. The host computer is an important part of the computer, which is the basic location for users to store data directly. Therefore, we must strengthen the host security, which will protect the security and privacy of user information. However, hackers, Trojans, worms and other network security threats often attack the computer, which has become an important threat to the application of network security. Therefore, we must strengthen the host network security protection, which will protect the host information from illegal network behavior. By ensuring the security of user host information, we can reduce the waste of resources. In the network security attack defense confrontation, both sides have natural asymmetry, which requires us to deal with network security threats. Through a variety of processing measures, we can protect the computer host security. Firstly, this paper analyzes the decision-making framework of network security threats and protection. Then, this paper puts forward the current mainstream treatment measures.

Keywords: Host Security Protection, Network Security Threats, Processing Measures

1. Introduction
In recent years, the main engine safety accidents occur frequently in our country, which has caused huge losses to our people's property safety. Therefore, China must strengthen the host security protection, which will improve the stable development of society [1]. However, due to the slow development of IT technology and database technology in China, the security and stability of network information in China are greatly threatened. Therefore, through independent security protection, we can strengthen the security of network system, which increases the technical difficulty of independent security protection [2]. At present, the means of information security attacks have gradually evolved to the direction of integration, which is also gradually developing towards diversification and complexity, such as viruses, worms, spam, botnets and so on. With the continuous growth of network attacks, the software and hardware vulnerabilities of hosts are gradually exploited by criminals, which has gradually formed a black industry chain of network attacks. With the application of information technology, new attack methods are emerging, which has caused many security threats, such as virtualization technology security, software and hardware attacks, network device attacks, web
application attacks, etc. Therefore, in the information network environment, we must innovate information security technology, which will enhance the host security protection [3].

2. Network security threat warning and defense decision framework

For different network security threats, the computer will implement corresponding defense decisions. This paper analyzes a threat early warning and real-time defense decision-making scenario. Through the model of attack defense confrontation, we can protect the host security. By solving the periodic and procedural threat warning, we can obtain the real-time defense decision-making scenario requirements, which will comprehensively improve the defense decision-making results. The decision framework of network security threat warning and defense is shown in Figure 1.

![Network security threat warning and defense decision framework](image)

Figure 1. Network security threat warning and defense decision-making framework.

3. Classification of network security threats

3.1. Network protocol

Network protocol is the rule that computer must obey when data exchange, which is also the most vulnerable place. The influence of human factors is not considered in the initial stage of network protocol formulation, which leads to a large number of security risks. At present, network protocol has
been optimized many times. However, the network protocol is still the most vulnerable place, there are the following attack methods. First, massive information bombardment, which will lead to computer failure. Under the normal information exchange request, the computer network will reply to the request. If the other party does not reply in time, the computer system will be in a waiting state for a long time. Therefore, the illegal elements use a short time to send a large number of requests to the computer, which will cause the whole system to be in a waiting state [4]. Therefore, the computer will not be able to maintain normal operation, which will cause user demand or system crash, such as tcpsyn denial of service, ICMP flooding attack, UDP flooding attack and so on. Second, modify the IP packets, which will lead to run errors in the packet parsing process. By modifying IP packets, criminals can achieve the purpose of data destruction [5].

3.2. System FLAW
System vulnerability is the existence of business logic errors or loopholes in the software design process, which will cause illegal elements to implant Trojan horse or virus. Through the system vulnerability, we will achieve the target computer data destruction or theft, such as windows PNP vulnerability, IIS IDQ vulnerability and so on. Through loopholes, users can access through special means, which will lead to illegal elements easily access data and steal [6].

3.3. User actions
User operation is one of the main sources of host security risks. Most network users in our country are lack of security knowledge. When the host computer is opened, the security of the host will be destroyed. By creating domain names similar to the user's target address, criminals can attract users to other web sites, which will gain the trust of the computer. In this way, the illegal elements will steal the user's personal account and password information. Through the software bundle installation, users have a great risk of embedding Trojan horse, virus, etc., which will achieve the purpose of user information destruction or theft [7, 8].

3.4. Trojan virus
Webpage hanging Trojan horse has become the most common means for attackers to quickly implant into the user's machine, which is the most important attack mode for network security. Trojan horse manufacturers continue to study new technologies, which will gradually get rid of the anti-virus tools. Traditional network worms can be implanted into computers through e-mail, Im, SNS and so on, which has gradually improved the concealment. Botnet is a transfer mode from IRC protocol to HTTP and various P2P protocols, which will enhance the concealment and robustness of Botnet. Through low frequency and shared attack mode, zombie transmission is more subtle.

3.5. Emerging wireless terminal attacks
With the rapid development of 5g, WiMAX, LTE and other wireless broadband technologies, PDA, wireless data card, smart phone and other mobile terminals will become the main target of hacker attacks. In addition to the traditional means of attack, many new means of attack have been developed, such as virus attack of mobile phone operating system, Trojan attack of wireless business, malicious broadcast of garbage phone, application worm of MMS, spam SMS, mobile phone information theft, SIM card reproduction, hacker attack, etc. Therefore, the way of wireless terminal attack brings great challenges to mobile terminals.

4. Network security technology

4.1. Trusted technology
Trusted technology is used to provide a secure and trusted environment from terminal to network system, which is a system engineering. Trusted technology mainly includes the following aspects: trusted computing, trusted object and trusted network. Among them, trusted computing introduces the
trusted architecture through the terminal hardware platform, which will improve the security of the terminal system. PC, server and mobile terminal are all entities of trusted computing. Trusted object is a way to identify the credibility of all effective entity objects in the network. By determining whether network services are needed, we can effectively control the propagation of untrusted objects. Among them, IP address, e-mail, web page, web address and so on are entities of trusted objects. Trusted network is a way to integrate security capability into network capability. By designing a secure network architecture, we can guarantee the security capability of the whole network. Various network devices and network elements are entities of trusted network.

4.2. Cloud security technology
Cloud security technology is a rising technology, which is based on user desktop / boundary device technology. Through the security processing ability, cloud security technology can be transferred to the data center as the core of security processing. Through centralized scheduling, we can improve the convenience, convenience and efficiency of users to enjoy security services. At present, cloud security technology is mainly divided into two categories, namely cloud computing security capability and virtualization cloud security technology. At present, UTM technology is a way to improve the efficiency of application layer security capability, which can improve the efficiency of network layer security capability. Through the cloud computing mode, we can transfer the bottleneck processing content to the cloud computing module, which will transform the long processing time of the device into short transmission. With UTM, we can greatly improve efficiency. Cloud computing can perfectly deal with the low efficiency of reputation evaluation system. The computer needs to process a lot of historical information, database and distributed processing technology, which will innovate information security technology, such as online antivirus, information security assessment center SOC, distributed IPS, etc.

4.3. DPI Technology
The Internet has entered the era of rich web applications, which has more responsibilities for the traditional network operators who provide network bandwidth. In addition to laying network channels, operators began to explore the application of network services. Therefore, DPI technology is more and more favored by network operators. In addition to detecting the quintuple information, DPI technology can also detect the payload and correlation of messages, which will realize the deep identification of messages. DPI technology can help network operators allocate network bandwidth resources more optimally. Therefore, we need to conduct in-depth security precautions against network attacks, which will bring positive effects to the fine operation of network services.

4.4. Web application security technology
The industrial chain of underground hackers has formed a system, which makes attackers focus more and more on Web application attacks. Therefore, the security of web applications is becoming a research hotspot in the field of information network security technology. Typical web application security technologies mainly include the following categories. First, web firewall. Web page is the main data source and user interface of the website. Web firewall establishes a security mechanism based on Web page security access control. We can enhance the security of web page system by checking the access restriction and legitimacy of web visitors. The main implementation methods of Web firewall are software firewall based on Web server and web hardware firewall based on gateway. Second, URL filtering. The Internet can provide rich applications, which has become a platform for spreading bad information, such as pornographic websites, violent websites, terrorist websites, etc. The URL filtering function can manage and filter the URLs of bad network resources. The number of bad websites on the Internet is huge and changing every day. Through the filter, URL can filter a variety of bad websites. Third, spam. E-mail has become the most commonly used network tool. Anti spam technology has long been valued by everyone. In addition to the traditional white list, blacklist, rule-based filtering email, source authentication technology, we have begun to apply new technologies,
such as content fingerprint analysis, email reputation evaluation, etc., which can be used to deal with e-mails such as pictures, advertisements and voice of bad pictures. Fourth, the webpage hangs the Trojan horse guard. Webpage hanging Trojan horse has become a very popular way of spreading Trojan horse, which has great harm. At present, many web security gateways have the ability to check and kill webpage hanging Trojan horse or control access to webpage hanging Trojan horse. In addition to network security tools, we can also improve the ability to prevent web pages from Trojan horses, such as updating system patches, unloading unsafe plug-ins, disabling scripts, running ActiveX controls, and implementing web reputation evaluation. In addition, we also have different Web attack prevention technologies for web viruses, phishing websites, spyware, etc.

5. Conclusion
Under the background of information age, data security has a significant impact on individuals and enterprises. Through the network security technology, we can protect the host security, which will better protect the host data information. At present, our country has already had the more mature host network security protection technology, which still needs us to strengthen the network security processing measures, which will make the host security get more rigorous protection. Therefore, in the information network environment, we must innovate information security technology, which will enhance the host security protection.

Acknowledgment
Supported by the high-end training project for teachers of higher vocational colleges in Jiangsu Province. Qinglan Project of Jiangsu Province. The 13th Five-Year Plan of Jiangsu Province :Research and Practice of the New Generation Information Technology Talent Training Model under the "1+X" Certificate System( D/2020/03/20).

References
[1] Fan Tanghe. Network security threats and Countermeasures of cloud computing [J]. Science and technology communication, 2015 (20): 80-84.
[2] Fang Binxing. Definition of Cyberspace Security [J]. Journal of network and information security, 2018, 1 (1): 1-6.
[3] Gong Jian, Zang Xiaodong, Su Qi, et al. Overview of network security situation awareness [J]. Acta software, 2017, 28 (4): 1010-1026.
[4] Ma Liqiang. How to effectively improve the level of computer network security in the information age [J]. Computer Engineering, 2011 (9): 79-83.
[5] Shi Leyi, Zhao junnan, Li Qin, et al. Analysis and Simulation of network deception defense strategy based on signaling game [J]. Journal of system simulation, 2016, 28 (2): 348-353.
[6] Tong Shunhai, Wu Dengfeng. Threats and prevention of network security in cloud computing environment [J]. Electronic technology and software engineering, 2015 (24): 40 - 43.
[7] Yao Ping, Li Hong. On the network security threats and Countermeasures of cloud computing [J]. Telecommunications Science, 2015 (02): 20-22.
[8] Yu Dingkun, Han Jihong. Signal game network security threat assessment method [J], Journal of Xi'an University of Electronic Science and technology, 2016, 43 (3): 137-143.