Research on the Quantitative Assessment and Security Measures of Hierarchical Network Security Threat Situation

Rui Mai, Mingzhu Wu*
Hainan College of Economics and Business, China, 571127

*Corresponding author e-mail: rkex28@163.com

Abstract. With the rapid development of modern network technology, technology not only changes people's life, but also breeds a variety of new problems. With the popularization of network application technology, various kinds of harmful means are emerging, and network security problems emerge in endlessly, among which information network security is the most prominent. This paper mainly describes the development and response methods of information security threats, analyzes the main attack modes and the evolution of information security threats, and analyzes the development direction of vulnerability detection technology that threatens the root of information security. Aiming at the security problem of school network, through analyzing all kinds of hidden dangers of network security, the best way is the hierarchical security solution. According to the implementation of the network security deployment cycle, security strategies are proposed from the network planning, network management and the use of network individuals.

Keywords: Quantitative Assessment, Security Measures, Hierarchical Network; Security Threat

1. Introduction
Campus network has now become an important infrastructure of educational informatization and an important guarantee for the sustainable development of schools. Each school has established its own campus network, which mostly involves teaching, scientific research, administrative management, foreign exchange, student information management and other network applications. If the campus network information is lost, it will be threatened by network security, and the school and students will suffer significant losses. Nowadays, with the rapid development of network technology, the configuration level of various computer hardware devices is very different [1]. The ability and level of users and managers are also your good and bad. There are many security risks, not only hardware security and software security, but also student information security. In order to ensure the normal and smooth development of school network services, we must pay attention to network security.
2. DDoS Attack
The earliest DDoS attack is based on ICMP Protocol. It uses multiple terminals to send Ping datagrams to the server at the same time, which eventually leads to the limit of the number of server connections and throughput, or consumes the computing resources of the server, and finally leads to the downtime of www. Later, with the gradual upgrade of cloud computing technology, the backplane bandwidth of the core server room increases, and the Ping datagram under ICMP alone can no longer realize the DDoS attack on the server. At the same time, a large number of virtual machine rooms and IDC rooms have also opened the DDoS redundancy pool. It is found that the data source of the centralized contract, that is, through the load control facilities, fully imports its traffic into the DDoS redundancy pool, ensuring the security of the machine room.

However, with the increase of the backplane bandwidth in the computer room, DDoS technology also advances. For example, using streaming media, repeatedly querying databases with large amount of data, increasing the number of connections and other means can carry out DDoS attacks against the bandwidth bottleneck of the cloud server room.

![Diagram of DDoS Attack Prevention Strategy](image-url)

**Figure 1.** DDoS Attack Prevention Strategy

Common virtual machine service rooms will be equipped with core load balancing devices after access routing and core switching, which directly serve the WWW host cluster. In addition, streaming media server cluster, data warehouse server cluster and app server cluster are generally equipped with special load balancing [2]. After the core load is balanced, the DDoS traffic pool is generally arranged to divert the possible DDoS attacks.

In addition, in order to avoid the bandwidth bottleneck caused by the export bandwidth of a single computer room, the general IDC service provider or virtual machine service provider will arrange multiple image computer rooms under multiple operators in multiple cities at home and abroad to provide a more reliable and highly available system.
3. ARP Attack

The biggest difference between ARP attack and DDoS attack is that DDoS attack can directly ignore a certain scale of DDoS attack while increasing system redundancy, but ARP attack has small amount of data, low system tolerance, small-scale ARP attack, or only one viral ARP attack node, which can lead to the paralysis of the whole LAN. ARP attacks focus on the industrial intranet or the private office intranet.

![ARP Attack Diagram](image)

**Figure 2.** 1toN Mode of ARP Attack

ARP attack is the earliest attack mode used to obtain the networking permission in the network with high degree of freedom, that is, under the premise of no permission to obtain the IP address or the IP address in the local area network is full, through repeatedly sending out ARP request, the system deprives the online host of the IP address arp binding, so that the attacker can get the ARP binding authorization after dropping the line. But at present, ARP attack may bring more serious consequences to LAN, such as using ARP to attack multiple IP addresses, or using ARP to attack gateway directly, which leads to instability and low availability of LAN as a whole.

In 1toN mode, the attacker only needs to obtain the control right of one host, and can use remote desktop, virus trojan, etc. to carry out ARP attack on all nodes in LAN including gateway. The result is the instability of the whole LAN.

Nto1 mode is to directly control multiple hosts in the LAN through the LAN virus with strong diffusion, and control these hosts to carry out ARP attack on key hosts or gateways. The result is the disconnection of the whole LAN.
4. Network Security Precautions

In order to prevent DDoS attacks, we should purchase load balancing, DDoS traffic pool and other expansion services as early as possible, especially global load balancing services. By adding resources such as image host and image data warehouse, and cooperating with various security related development services, IDC host can be used with relatively complete security guarantee. In fact, although bat and other application service providers have established their own IDC rooms, many large-scale application service providers, such as TMD enterprises, also operate in IDC host communities. They have purchased more security services, which makes them obtain higher security.

Static ARP can prevent ARP attack to the maximum extent, and make the attacker drop his own line, so as to ensure that the LAN system will not develop into more serious consequences due to ARP attack to a certain extent. However, the static ARP will bring more tedious workload to the LAN management. When adding, removing and migrating hosts, the LAN administrator must manually change the static ARP table to re access the hosts. And if the LAN administrator misoperates, it may cause a large area LAN fault, and this fault is difficult to troubleshoot, so that the system recovery time is affected.

By building ARP server and introducing ARP intelligent AI management system, the equivalent dynamic ARP management can be realized in static ARP LAN system. At present, most ARP servers need users to install the client system on the host terminal [3]. The login user name and password assigned by the client system to the end user will automatically send the ARP application information to the ARP server. The ARP server will configure a new ARP table for users and update the relevant ARP table content according to the location change or MAC address change of the host.

Figure 3. Nto1 Mode of ARP Attack
For the LAN administrator, the update of ARP table must be done manually to the management of user login authorization. The difficulty and complexity of management are relatively reduced, and high-quality static ARP management can be carried out continuously.[4]

5. Summary
In a word, for the DDoS risk faced by the campus network, the security investment of the server is essential. Simply compressing the security related investment of the server may bring significant security loopholes to the system.

The ARP management server mentioned above can effectively avoid the loss of LAN function when ARP attack occurs. In addition to the ARP management server, an internal port monitoring system is set up to pre scan the vulnerability of each host in the local area network at any time, and immediately rectify the problems found. ACL system can control host behavior. On the one hand, it assists ARP management server to set ARP static binding.

Once ARP attack occurs, it will cause great trouble to LAN. But in the analysis of this paper, any LAN system has the ability to completely prevent ARP attacks, and even does not give ARP attackers the opportunity to build a meat machine environment. So as long as the operation is reasonable and the planning is scientific, the LAN can realize the overall security against ARP attacks.

6. Reference
[1] Maira R. Monteiro, Gabriel F. Alvarenga, Yuri R. Rodrigues, A.C. Zambroni de Souza, B.I. L. Lopes, Mauricio C. Passaro, Morad Abdelaziz. Network partitioning in coherent areas of static voltage stability applied to security region enhancement[J]. International Journal of Electrical Power and Energy Systems, 2020, 117:.

[2] Avleen Kaur Malhi, Shalini Batra, Husanbir Singh Pannu. Security of vehicular ad-hoc networks: A comprehensive survey[J]. Computers & Security, 2020, 89:.

[3] Ali Parizad, Konstadinos Hatziadoniu. Security/stability-based Pareto optimal solution for distribution networks planning implementing NSGAII/FDMT[J]. Energy, 2020, 192:.

[4] Xiaoheng Zhang, Doudou Li. Research on E-commerce Logistic Satisfaction Based on TOPSIS Method. International Journal of Frontiers in Sociology (2019), Vol. 1, Issue 1: 12-22.