The Border Attack Defense System is Software-Based

Rui Wang1,* , Yinxian Chang2, Lei Ma1, Hao Zhang1, Xin Liu1, Jianfei Chen1, Donglan Liu1, Yong Zhang1, Bing Su1
1State Grid Shandong Electric Power Electric Power Research Institute, China, 250000
2State Grid Shandong Electric Power Company, China, 250000
3Powered By Dechnic Co., Ltd., China, 250000

*Corresponding author e-mail: wangrui@sgcc.com.cn

Abstract. Now the computer has been completely towards the public, the network in daily life is more and more widely used, but at the same time, the potential network security problems are also more and more serious. Some sophisticated computer people in order to make money, crack other personal users or company information, a variety of network attacks one after another. Cyber attack has become an extremely feared existence for ordinary people because of its wide range of attacks, strong attack force and obvious hiding effect, which seriously threatens the security of personal information network. If attacked by this kind of attack, the loss borne by each person or company is immeasurable. In order to maintain network security, the defense system is also improving day by day, and finally presents software. This paper mainly makes a detailed understanding of the border attack and defense system, and analyzes the main reasons and inevitability of the software of the border attack and defense system.

Keywords: Boundary Attack, Defense System, Software

1. Development background

1.1. Understanding of border defense

Border defense is the concept of anti-virus technology first put forward by domestic security defense enterprises. This technology has been applied continuously in the past few years. Compared with the traditional concept of anti-virus technology, border defense is different in that ---- border defense emphasizes that the computer is completely free from virus attack is the most secure solution. As long as it is through the outside illegal program to carry out illegal monitoring of the selected computer, even if the virus has not yet run, this situation will be judged as safe or unsafe, so as to bring security for the protected computer to the greatest extent, reduce or even avoid loss. The specific steps for border defense are as follows:

First, a file enters the PC by downloading, copying, installing, etc., and then triggers border defense on the way to the PC. Then, border defense determines whether the file has content or not, passes the border if the file is empty, and prohibits the file if it has content [1]. Or if it is the file upload cloud identification of the cloud, because the cloud has a strong defense, the identification of a scanning,
appraisal to scan files, if unable to determine the artificial, then eventually return results by boundary or prohibit operation, such as the border defense is pretend to be normal software virus fool, but found that file has a virus in the system runtime behavior starts the defense system, and then killing virus, and then repair the system.

1.2. Understanding of border attacks
In the past, people set up the network era for sharing resources, computers all over the world are linked into a network, at the same time, security has become a problem. Because on the Internet, there's no way to know how accurate other people are. More and more insecure factors such as leaks, attacks, viruses and so on make it difficult for network administrators to be quiet. Because the Internet is a world class network of people, there are all kinds of unknown forces and groups on the Internet. A border attack is when someone enters your network through the Internet, tampers with your private data, breaks the network system, and causes the network to crash. Most of these attacks are active and purposeful.

1.3. Understanding of defense systems
Defense system is an organic whole composed of defense elements such as combat force planning, camp division, ammunition distribution, logistics support, and so on. It is the core information of defense operations. Whatever belongs to the defense system, should be composed of the above elements, the more complete the defense system, the more powerful the defense ability.

1.4. Boundary protection technology
Since the birth of the Internet, there has been an interconnected network. In order to protect the security of the network, people have invented two kinds of protection technology, namely firewall and gateway technology. The network boundary has always been the forefront of the attack and defense confrontation, so the importance of its protection is self-evident. Firewall is a network isolation or segment of an ecological isolation, because each segment of the connection between the mouth is through a router connected, if want to limit between part of the network segment is not connected to each other, or have under certain conditions, by the operating personnel to allow circumstances connected to each other, because of this demand, in life there is the access control technology, then a firewall [2-3]. To sum up, at the beginning of its formation, the firewall is just a kind of isolation technology walking between impassable gateways. However, a firewall can only solve a protection, but when we encounter a variety of virus invasion, will only be praying praying arms when the car, so, technical personnel and thought of another method ---- use multiple firewalls. Since a firewall can solve a kind of virus invasion, then, in theory, multiple firewalls can block the invasion of multiple viruses, while the security of multiple security gateways must be higher than the firewall. It can resist all kinds of common intrusions and viruses. But most of the gateway is determined by the characteristics of the invading virus identification to confirm the invading, fast this way, will not bring significant security hidden danger, but also has its own huge defects, first of all, the application characteristics of the updated generally faster, the latest features are hard to find, so the gateway to feature database upgrade in a timely manner; Secondly, many hacker attacks use communication, a little infiltration, take circuitous tactics, no obvious characteristics, security gateway for this kind of threat is not much effect.

2. Construction of border defense system
Nowadays, with the continuous development of the network and science and technology, online activities have become a big new business opportunities. Many small and medium-sized enterprises are slowly moving towards digital transformation. In the transformation process of most enterprises, numerous new security vulnerabilities have emerged, which has brought a lot of hidden dangers to the security problems of enterprises. In order to effectively avoid or find, solve this problem, each enterprise has also built a defense system. As we all know, the defense needs to consider the security
point, and the border is the core of the network defense, must be a complete protection of the border [4]. The construction of the border defense system is mainly divided into three steps, namely, prediction, defense and inspection. (Figure 1)

![Figure 1. Three steps in the construction of border defense system]

Anticipation: that is, for the operators to face the threat of the virus in advance of a detailed understanding, so as to carry out a very targeted defense.

Defense: After predicting the type of incoming virus threat, the operator needs to deploy the threat defense. When a virus attack occurs, the previous defense deployment can effectively protect against it. This is the core part of the whole system, if the defense fails, the operators can only face their own business to be hit, confidential business stolen by others and powerless.

Inspection: in the face of the security system has taken the defense, it is necessary to confirm whether it is completely cleared, whether there are hidden dangers, and then the source of the virus attack is the target for accurate positioning and counterattack. Make the personnel under attack to carry out the corresponding analysis, and take timely and effective measures to minimize the loss.

3. Software of defense system

3.1. The embodiment of software
System software-based definition: System software refers to a set of elements in a certain form, including data display, data processing, and the connection of corresponding relations. The processing of data means the deep processing of data [5-6]. Component is the core to be processed. The connection of relation means the combination and connection of different parts in the set, which has a certain hierarchical relationship.

Now, with the popularization of computers and the rapid development of the network, the importance of information security is constantly reflected everywhere. And when we have a computer, open the software, found a lot of security software, antivirus software, few people write their own security software or specifically to find someone to write a. The border defence system is truly software-based.

3.2. Reasons for softwareization
(1) Advantages of software
Custom interface: as a software, as long as the relevant personnel will download the software, the software interface is connected to the personal private, they can freely change the interface display, showing their own favorite style, so as to achieve personalized. In this way, operators can easily make a variety of styles according to their own needs, so as to establish their own needs of information generation system.

Convenient operation: the boundary protection system software, the operator does not need any programming knowledge, can be in any place, any time, any object can be protected [7-8]. And the software automatically records the time and location of the intercepted viruses, preventing the operator
from having to view or print a list of the intercepted viruses. When printing a list, the number of columns in the list and the contents of the list are freely selected by the operator. For example, the operator can combine the list at will according to their own wishes or requirements, and display it to others to view according to their own wishes.

Data stability: the software uses the database, the database is relatively stable and safe, suitable for the user with huge amount of data and high stability.

Good expansibility: the software has expansibility, the software itself can be easily modified according to the needs of users, but also with the increase of users' needs, the scale and scope of its own to expand and diverge again, to ensure the personalized software.

![Advantages of software](image)

**Figure 2. Advantages of software**

(2) Specific life reasons

First of all, the development of modern Chinese society is still in the unbalanced and inadequate development. If someone were to write a border protection system, the cost would be a huge amount of money. In China, there is no shortage of economic backwardness among many computer-owning households. And the free use of the software has brought them a big convenience. By downloading the software, they only need to open the scan every time, greatly reducing the overhead. Second, most of the software is developed by the company, for some software companies, software download Numbers corresponding to the amount of their marketing, linked to their profit directly, so they will try every way, to increase exposure of software, meanwhile, the software of exposure rate increases, the number of download nature also is increased. Still have, the border defense attack defense system software, greatly facilitated the application of the student party [9-10]. As a college student in school, computer is essential, and most of the computers are stored to put their own learning materials, once the computer is attacked, learning materials and personal information lost, will bring endless trouble. First of all, learning materials are lost, you may need to start all over again, which greatly increases your pressure. On the other hand, personal information loss, when you meet some large exams, if the other side deliberately against you, he can modify or cancel your examination registration at any time, seriously affect your footsteps. Every year, tens of thousands of engineering freshmen are enrolled across the country, many of whom specialize in software development. For this part of the students, their employment is mostly about software development. Without software development, they would be out of work. In a word, the softwareization of the border attack defense system is an inevitable trend.

4. Conclusion

With the continuous development of high and new technology, the Internet era has come, and the network has become an indispensable part of people. At the same time, the network security problem is also imminent. In response, thousands of border attack defense systems have been introduced. With the increase of people's demand, the border attack defense system is also gradually software-oriented, more to meet the needs of the public. This paper mainly makes a detailed understanding of the border attack and defense system, and analyzes the main reasons and inevitability of the software of the border attack and defense system.
References

[1] Huang Wei, Liang Hongliang, Hu Zhengming, et al. VoIP Network Boundary Attack Protection System Journal of Tsinghua University (Natural Science Edition), 2009, 049(0 z2):2215-2221.

[2] Gao Yan, Zhang Rui. Design and Implementation of Border Protection Equipment for Signaling Network No.7 Based on Rule and [J]. Detection Technology Communications technology (phase 7):943-949.

[3] Bai Shengjiang. A Study on the Border Protection System of Active Military Network [D]. Xi'an University of Electronic Science and Technology.

[4] Zhang Bo, Zhang Tao, Ma Yuanyuan, et al. A Cooperative Defense Method and System for Boundary Security of Power Network: CN109218292A[P]. 2019.

[5] Bao Shikui, Ning Yuqin, Jia Zhigang. Construction and J. of Network Security Defense System Science and Technology Advisory Bulletin, 2007, 000(012):6-6.

[6] Zheng Xianju. DDoS Attack Analysis and Defense Methods [D]. and University of Electronic Science and Technology.

[7] Xiao Haohang. Application of Third-party Boundary Security Protection Technology in Computer Network [J]. Technology and Markets, 2016(10):93-93.

[8] Zhang Jianghong. Design and implementation of a distributed boundary protection system Sichuan University, 2007.

[9] Li Yanjun, Zhang Guoqing, Shen Subin. A construction method of domain traceability global network security system:.

[10] Xie Dongqing, Qike, Zhou Zaihong, etc. A defense method for distributed denial of service attacks:.