Research on Network Risk Assessment Method Based on Dynamic Attack Behavior

Weiwei Lin[1,2]

[1]School of Electronic and Information Engineering, Fuqing Branch of Fujian Normal University, Fuzhou, Fujian, 350300, China

[2]Engineering Research Center for ICH Digitalization and Multi-source Information Fusion, Fujian Province University, Fuzhou, Fujian, 350300, China

Keywords: Network Risk Assessment; Dynamic Attack; Network Technology

Abstract: Network attacks are frequently faced by modern network systems. In order to improve the security and stability of the website, it is necessary to conduct risk assessment through the network to simulate the dynamic behavior of attack events. It is necessary to test the network's anti-risk ability. This is also the modern development. As an emerging technology, this paper makes some research on the network risk assessment method based on dynamic attack behavior.

1. Introduction

Using the dynamic network change concept to simulate events and conduct network risk assessment tests. A new method developed on the basis of conventional network risk assessment research work. This method can be used to complete the test procedures through the framework construction method. The tasks and objectives are located to effectively complete the risk assessment. Compared with the traditional method, this method can restore the complex, dynamic and diversified characteristics of the network attack behavior, and can test the network security vulnerabilities from all angles to comprehensively and accurately judge the network[1]. The health, based on the simulation of dynamic attack behavior, can also summarize and analyze the time characteristics of cyber attacks, so as to plan to make time-to-face response defense measures, which is an advantage that early risk assessment analysis does not have, so talk about modern The network risk assessment method under dynamic attack behavior is of great significance to the development of the industry[2].

The network risk assessment method in the current dynamic attack behavior is mainly constructed by using the framework. Under the framework construction, a variety of rule bases are formed, and the rule base is used for process derivation, thereby fully exposing the deficiencies in the network security construction. With the development of time, the formal rule graphics have become various types of model methods such as attack graph method, state transition method, attack tree method and privilege graph method[3]. Different methods can be used to face the network for risk assessment.

2. The Principle of Network Risk Assessment Based on Dynamic Attack Behavior

The construction of the network risk assessment method based on dynamic attack behavior fully combines the advantages of qualitative research and quantitative research under the early static research[4]. Because the characteristics of the early static research method determine that qualitative and quantitative are difficult to integrate, when analyzing, No matter which one is used, it is impossible to complete the evaluation problem of the system over time when it is attacked, which leads to large distortion of the result. Therefore, under this demand, by combining the advantages of both, and integrating with time The curve research has developed a more comprehensive network risk assessment method under dynamic attack behavior.

Considering that the large-scale network itself is characterized by a wide range and many channels, it also adopts multiple defense systems in defense. In order to improve the attack success

  DOI: 10.25236/mmmce.2019.090

rate, attackers often need to crack the network defense through step-by-step testing. In the early stage of the cyberattack, as long as the curve of the attack behavior over time is clearly defined, it can better defend the follow-up defense. Based on this, relevant experts and scholars introduce a timeline to dynamically cyber security risk assessment. This lays a foundation for establishing a good dynamic access relational network[5]. By making the network attack behavior public, it can greatly enhance the defense construction of the network attacker, which effectively ensures the security construction of the network.

3. Research on Dynamic Network Risk Assessment Method Based on Attack Events

3.1. Implementation of risk assessment method based on abstract graph method

According to the analysis of the attack model in the network security risk assessment, if a large-scale study is conducted from a long time, it may be difficult to achieve due to the influence of some factors, such as amplified noise, but at the same time, it is found that If the scope of the study is limited to a period of time, the results obtained will be relatively stable. It is a good feasibility analysis to convert long-term attack pattern changes into multi-segment stable research conditions. Through direct analysis of different stable segments, Get a clearer study of the impact of attacks on network networks. In addition, different stable segments may also have certain common characteristics, which can be obtained through scientific and effective analysis methods, which can comprehensively and comprehensively reflect the changes and rules of network changes[6].

When the network segmentation is selected, the original calculation results can be integrated and analyzed to obtain different stable segments. When the segmentation is performed, the sliding window can be observed to determine a more accurate reference. Numerical values, and the high values are trimmed, and the low values are smoothed[7]. In order to obtain a more stable evolutionary segment, the actual data is more realistic. Consider using the approximate graph extraction method to process the data. The execution flow of the processing method is considered. Yes, the stable processing segment is processed separately by using the conventional processing method and the approximation graph method, and the obtained results are compared, and the common points of the two are retained, and then the comparative analysis is performed for different points, and the reasons are often dig deep, which is often It involves some vulnerable vulnerabilities.

3.2. Risk assessment method for Bayesian attack graph

The Bayesian attack graph method can better reflect the state of each element stage and the causal relationship between each other. When using this method for evaluation, the framework construction must still be carried out first. The difference is that the method not only indicates the node, but also It is indicated that the probability of occurrence of state transition between causality is evaluated. When using Bayesian attack graph for evaluation test, node probability estimation must be performed before the next step can be deduced[8]. Therefore, using this method for evaluation has a good data foundation. Repeated calculations can be repeated, and the results are also very intuitive and reliable. Moreover, this method can determine the more vulnerable attacks by probability assessment, so that targeted and targeted network defense construction can be made, which can be well reduced. Defense construction costs.

In the dynamic risk assessment, in order to make the probability calculation of the Bayesian attack graph better to take advantage of the reliability, the following optimizations are also made to the probability calculation: when the same type of resources exist in different network resource nodes, the first The difficulty assessment of the attacked point increases the chance of attacking the same point. For example, if TCP is used in multiple nodes, then after the first TCP is broken, the subsequent TCP is also easily attacked by the attacker in the same way, so A certain numerical correction is made to the probability of the Bayesian attack graph to increase the probability that subsequent TCPs are attacked. In addition, on the similar nodes, by analyzing the attacker's means, the attacker's behavior characteristics are found, thereby predicting the attacker's subsequent attack

route, and realizing a more realistic guiding risk assessment, such as determining the maximum according to the characteristics of the attacker. Possible attack paths, and then interception on multiple paths, can effectively improve the security level of the network[9].

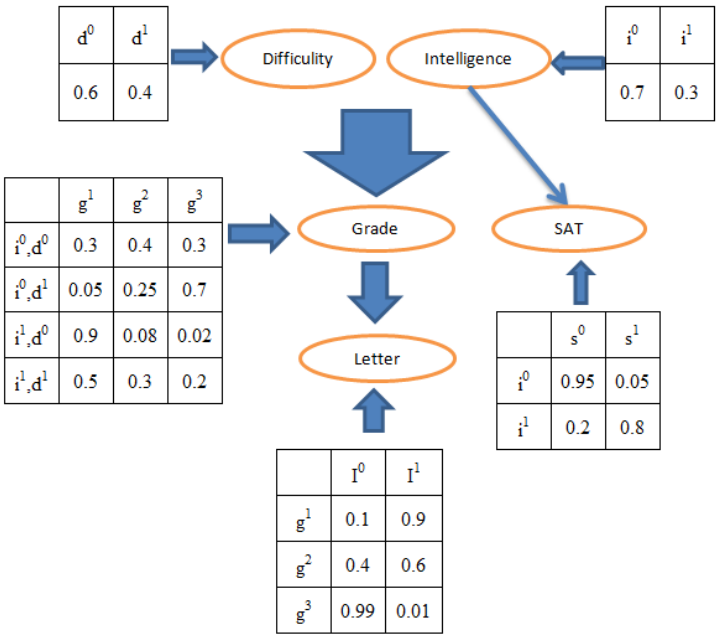

Fig.1. Bayesian attack diagram

4. Analysis of the Key Points of the Framework under the Risk Assessment System

Through the analysis of the above methods, it can be known that the analysis method based on dynamic attack events has a good advantage, but the difficulty and complexity of operation are also greatly improved compared with static analysis. Therefore, dynamic network risk assessment based on attack events is carried out. When constructing the framework, it is necessary to conduct feasibility analysis first to ensure that the framework has practical guiding effects on the current risk analysis. In the specific construction links, the following points should be noted:

First, in the framework simulation, each node and path should have a more scientific and reliable simulation construction method. The initial data measurement and numerical change methods should be well matched with the actual network nodes for construction, especially in the relatively fragile In the construction of nodes, a comprehensive analysis should be carried out from the configuration data processing method of the facility. In the analysis of the multi-segment attack graph, the advantages of the sliding window can be fully utilized for analysis[10].

Second, in the data processing, you can not only use pure mathematics for data processing, but also be good at analyzing the actual device operation mode. The data points with large fluctuations are often the crux of the problem.

Third, after getting a more complete data calculation, how to restore it to risk assessment, how to provide guidance for the actual network security construction needs to have a more comprehensive guidance construction plan, it is best to form a targeted , systematic construction plan.

Fourth, make full use of the dynamic assessment of time-based attack characteristics, so that data collection and analysis can be completed quickly at a specific time, thus effectively reducing the cost control problem of network risk assessment.

5. Conclusion

The dynamic network risk assessment method based on attack events is of great significance to the continuous development and upgrade of modern computer network security management. When

conducting network risk assessment, it is necessary not only to combine existing experience to conduct research, but also to be good at combining actual and in-depth mining. The causal relationship between more factors, thus achieving faster and more effective network system security defense, is a higher requirement that relevant experts and scholars should put forward to themselves.

Acknowledgement

(1) This work was supported by the Natural Science Foundation of Fujian Province, China; Research on network risk assessment method based on dynamic attack behavior (Grant No. 2019J01889).

(2) This work was supported by the Education-Scientific research Project for Middle-aged and Young of Fujian Province, China; Research on analysis system of malicious code based on API relevance (Grant No. JT180626).

References

[1] JAJODIAS, GHOSH AK, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats. Springer Ebooks, 2011: 54.

[2] Cai Guilin, Wang Baosheng, Wang Tianzuo, et al. Research Progress of Mobile Target Defense Technology. Journal of Computer Research and Development, 2016, 53(5): 968-987.

[3] Whitley J N, Phan R C W, Wang J, et al. Attribution of attack trees. Computers & Electrical Engineering, 2011, 37(4): 624-628.

[4] Dalton Ii GC, Edge KS, Mills RF, et al. Analysing security risks in computer and radio frequency identification (RFID) networks using attack and protection trees . International Journal of Security and Networks, 2010, 5 (2 /3): 87-95.

[5] Ammann P, Pamula J, Ritchey R, et al. A host-based approach to network attack chaining analysis. Computer Security Applications Conference. 2005: 72-84.

[6] Ye Wei, Guo Yuanbo, Wang Yidong, et al. Review of application research of attack graph technology. Transactions of Communications, 2017, 38(11): 121-132.

[7] Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 61-74.

[8] Miehling E, Rasouli M, Teneketzis D. Optimal defense policies for partially observable spreading processes on bayesian attack graphs. ACMWorkshop on Moving Target Defense. 2015: 67-76.

[9] Nguyen T H, Wright M, Wellman M P, et al. Multi-stage attack graph security games: heuristic strategies, with empirical game-theoretic analysis. ACM Workshop on Moving Target Defense. 2017: 87-97.

[10] Bopche G S, Mehtre B M. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks. Computers & Security, 2017, 64: 16-43.