Research on Diversity Characteristics of Mimic Defense Gateway Business Environment

Jun Yu\textsuperscript{a}, Guangxin Zhu\textsuperscript{b}, Lin Wang\textsuperscript{c}, Mingjie Xu\textsuperscript{d} and Haiyang Chen\textsuperscript{e}

State Grid Electric Power Research Institute, Nanjing, 210000, China

\textsuperscript{a}yujun@sgepri.sgcc.com.cn, \textsuperscript{b}zhuguangxin@sgepri.sgcc.com.cn, \textsuperscript{c}wanglin18@sgepri.sgcc.com.cn, \textsuperscript{d}xumingjie@sgepri.sgcc.com.cn, \textsuperscript{e}chenhaiyang@sgepri.sgcc.com.cn

Abstract. This paper introduces the security problem of SDN gateway based on software-defined network, compares the mimicry security controller model of dynamic heterogeneous redundancy, the mimicry network scheduling and security mechanism, and the advantages and disadvantages of ontology-based network mimic defense system security modeling, and introduced the future research work.

1. Introduction

The Software Defined Network (SDN) realizes the separation of control and data forwarding through programmable ideas. The advantage of this design is that it makes it easier and more efficient to add higher levels of routing, traffic engineering. As a mainstream SDN solution, Open Flow controllers centrally control the popularity of the entire network. This logic centrally controls network routing and forwarding to increase the efficiency of the switch. However, since most controllers focus on network transmission performance at the beginning of development and design, regardless of security factors, this centralized control mode faces enormous security problems, and the controller acts as a network "command." The control center has become the main target of attackers launching cyber-attacks [1-2].

In order to solve the above problems of the SDN controller and ensure the security of the SDN network, the researchers conducted a lot of theoretical research and engineering practice. The design of the controller is mainly divided into two aspects. One is to improve the security of existing controllers, such as Fortnox [3] and SE floodlights [4]. Although these studies can improve the security of the controller to a certain extent, the improvement scheme is to improve and expand the corresponding security module of the original controller, so it is inevitably affected by the original controller design idea and programming language. Secondly, a new type of safety controller is designed. Because most controllers are designed and developed to implement the logic functions of the controller, such as message processing and processing rules. The security of the controller itself has not received enough attention, some researchers suggest designing new security controllers, such as panel [5] and rosemary [6]. Designing a new controller avoids the limitations of the improved solution patch, but like the previous solution, these solutions cannot avoid the single point problem of the SDN controller as a centralized control node. At the same time, due to unknown and unavoidable natural backdoor vulnerabilities, the safety controller will generate new safety risks based on these two design options. Although the security of the controller can be developed after the repair, by fixing the yoke of the suffocation, the problem in the security SDN control layer cannot be fundamentally solved. Simulated
defense is a new defense method. It mimics the phenomenon of imitation in the biological world. It is characterized by dynamics, heterogeneity and diversity. By preventing an attacker from gaining information and destroying the attack path, the attacker can be effectively protected. Due to the introduction of the above features, the research methods of traditional information systems cannot be fully applied to the security of the simulation defense system. Based on the application of simulation defense technology, the architecture of SDN control layer with endogenous security features is constructed, and its scheduling decision mechanism is studied. It helps to promote the development of simulation security defense technology theory, and helps to promote SDN network security and simulation defense in engineering.

2. Related work

2.1. Mimic Defense Mechanism
Simulation security and defense technology is a security strategy with severely asymmetric network attack costs and defense costs. Through the heterogeneity, diversity, similarity and uniformity of the system, dynamic and randomness are used to change the static and certainty of the system, and non-similar space is used to prevent or destroy the network attack, thus realizing the security risk of the system. Control requirements.

In particular, analog protection is a core feature consisting of heterogeneous and similar actuators. It uses dynamic redundant structures to implement dynamic and random structures. The detection or prediction of the attacker's difficulty in defense behavior and features will grow non-linearly, which makes the complexity of the system unprecedented, making it difficult for attackers to exploit system vulnerabilities [7]. The simulation defense includes multiple scheduling decisions, random/dynamic, iterative superposition, differential design and dynamic heterogeneous redundant structure, which together constitute the overall defense function of the simulation defense system.

2.2. Active Defense Technology
The traditional cyberspace security defense is mainly to strengthen the external security of the target system, detect and eliminate known threats. In order to change this situation, various active defense techniques have been proposed and studied, including Mobile Target Defense (MTD) [8] and Byzantine Fault Tolerant System [9]. The core idea is to build a dynamic, heterogeneous, and uncertain network target environment, improve the attacker's attack difficulty, and use the system's randomness and unpredictability to defend against network attacks. In the storage system, the Byzantine system design is mainly divided into state machine Byzantine agreement and legal Byzantine agreement. The main difference between the two protocols is that the former requires the serial number of all requests, and all requests must be executed in order. The latter does not require the requested serial number.

3. Development trend
At the present stage, foreign related researches put forward mobile target defense (MTD) [10] as the active defense to change the network security mode. Compared with traditional security methods, they have great innovation in security mechanism. The difference lies in that the former pays attention to dynamics, increases the system uncertainty through the attack surface theory, weakens the attacker's detection advantage, and improves the attack ability. This paper discusses the basis of simulation defense theory, and designs a security defense mechanism based on SDN controller, so as to improve the ability of network control layer to resist network attack.

4. Proposed technology

4.1. Dynamic Heterogeneous Redundant Mimetic Security Controller Model
This heterogeneity includes both hardware and operating system levels. Considering the dynamic changes of nodes and network structure in the controller cluster, the active and passive dynamic
scheduling of controller cluster elements is realized through a certain security scheduling mechanism, which improves the uncertainty of the system to attackers. Client security requires dynamically expanding controller clusters for increased scalability. Fault tolerance. The dynamic implementation of the defense model is a key module of the simulation. Through a certain scheduling strategy, the dynamic scheduling of the controller executor is realized, and the dynamic, diversity and uncertainty of the controller execution cluster are improved, and combined with the control in the scheduling resource pool. Heterogeneous nodes implement dynamic defense to improve security. The controller processes the request data and the result package. Use the stream mod information to return to the client. As a forwarding module, the server agent has the characteristics of transparent transmission, and sets a FIFO queue for each data processing to ensure the sequential transmission of data. After returning the processing result, the client determines that the received consistent F + 1 response is the correct processing result.

Figure 1. System workflow.

In the security controller architecture model based on the dynamic heterogeneous redundancy idea, the controller cluster configures a corresponding number of control nodes according to the security requirements of the controlled SDN switch. Different software and hardware types are used between nodes. Keep the maximum number of nodes. Independent. Under the architecture model, the output of the control layer is always judged by the service agent until the result is consistent. In addition, for a destructive attacker, in the timeout setting, the output delay or non-output caused by the attack will be regarded as null. In the communication negotiation process, the null value obtained by the algorithm analysis will be invalid. This role can be avoided to avoid the effects of destructive attackers.

4.2. Mimetic Network Scheduling and Security Mechanism

The dynamic heterogeneous redundancy model based on the simulation defense idea is expected to realize the threat perception of independent attack features through the heterogeneous redundant multi-mode voting framework. Changing the similarity and homogeneity of the defense environment is heterogeneous and diverse; randomness and randomness change static and random. Using the deterministic defense behavior of the target system and the given vector space multi-mode arbitration mechanism, the difficulty of coordinated attacks under non-cooperative conditions is improved. Use intensive architecture technology to enhance the flexibility of the target object service function, and use the "unrestricted attribute defense" of defense behavior and environment to reject the intentional attack of the target system vulnerability backdoor. Ultimately, these goals can be achieved through integrated integration architecture techniques. The structure of DHR is shown in Figure 2.
The architecture consists of input agents, heterogeneous sets, dynamic scheduling algorithms, executable sets, and multi-mode voters. As success. The input agent is responsible for assigning input to each executable that is currently running. The voter makes many decisions on the output vectors generated by all executables to get the final output.

The theoretical need greatly reduces the likelihood that different types of executables will have the same vulnerability. Even if there are common or different vulnerabilities in various executable files, it is difficult for the relevant executors to fully cooperate under a wide range of dynamic non-cooperative conditions. This is because the multi-mode advantage chain forces any non-cooperative attack mechanism to fail, successfully escapes, and even achieves sustainable escape. Without repeated testing, it is difficult to achieve dynamic multi-target goals. Cooperative attack. Output vector. In addition, the multi-pattern rule-based strategy scheduling and the multi-reverse dynamic feedback negative feedback mechanism have a strong inhibitory effect on the anomalies caused by repeated experiments. The dynamic heterogeneous redundancy model of simulation defense can effectively improve the intrusion tolerance and reliability of the system and greatly improve the security performance of the system.

First, each controller can independently complete the OpenFlow messages reported by the underlying switch assigned by the scheduler. Although different programming languages or design ideas are used, the decision is made and the corresponding processing results are given. Second, the controllers in our analog controller pool are independent of each other and do not have east-west communication capabilities. Finally, in our design, there is no need to modify the original core functional modules of each controller, so it is non-invasive and easy to develop, add, and extend new controllers.

The basic function of a scheduler is to periodically select a new set of active state controllers from the simulated controller pool based on scheduling policies. When a suspicious controller is found or a transition phase is reached, the scheduler selects a trusted controller from the controller pool to replace the suspected active state controller based on a predefined scheduling policy. In addition, an odd number
of controllers are chosen as active state controllers because a large number of mediation mechanisms are usually used.

The core function of the arbitrator is to comprehensively judge the response results returned by multiple controllers according to the predetermined decision mechanism, select the most reliable result as the final result, and transmit it to the underlying switch. Part of the data is the suspicious controller message sent by the arbitrator. The scheduler invokes historical data to select the most trusted controller. Part of the data is the information that the controller registers with the manager to manage when it joins the controller pool.

4.3. Security Modeling of Network Mimetic Defense System Based On Ontology

According to the principle of simulation defense, the main simulation ontology classes and their semantics are as follows: The simulation mechanism can be used to implement the information system components at all levels. MDB: mim defender is an information system component that includes multiple dynamic heterogeneous redundant actuators. Its core functions are realized through dynamic heterogeneous redundancy mechanism and multi-mode control mechanism. Simulation defense of dynamic heterogeneous redundant actuators can also be realized by simulation mechanism, that is, simulation defense allows simulators to form new simulators by stacking and nesting themselves. Dynamic heterogeneous redundant execution DHRE: a group of heterogeneous information system components with equal output and redundant functions, providing external function Security vulnerability: a security vulnerability, vulnerability, or backdoor in an information component. Attackers can exploit security vulnerabilities to break the security properties of information components or even gain control. Available security vulnerability ESV: the simulated defense system has one or more attack paths from the attack surface. Security holes in the attack path become available security holes.

Using ontology modeling method to simulate the CMD of the defense system can not only clearly describe the relationship between CMD and DHRE internal components, but also include security vulnerabilities and attack surface and other security vulnerabilities. Test examples show that this model complements the corresponding security attack and defense rules written by SWRL, and completes the security judgment of the ontology system effectively by means of logical reasoning.

5. Conclusion

In this paper, three mimic defense security technologies based on software-defined networks are introduced in detail. Through the research, it is found that the mimic security controller model based on dynamic heterogeneous redundancy improves the uncertainty of the system against attackers and reduces the probability of attack infection, while the mimic network The scheduling and security mechanism intercepts the attacker's use of system detection and attack results in the attack chain, reduces the probability of attack success, guarantees the security of the SDN control layer, and improves the security of the SDN network. The ontology-based network mimicry defense system security modeling the method effectively completes the security judgment of the CMD system.

Acknowledgments

This work was financially supported by the science and technology project of State Grid Corporation of China: "Research and application of Mimic Defense Gateway applied to web application for power grid" (Grand No. 52110118001F).

References

[1] Diego K, Fernando MVR, Paulo V. Towards secure and dependable software-defined networks [C]//Proc of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. New York: ACM Press, 2013: 55 - 60.

[2] Scott-Hayward S, Natarajan S, Sezer S. A survey of security in software defined networks [J]. IEEE Communications Survey & Tutorials, 2016, 18 (1): 623 - 654.
[3] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for OpenFlow networks," 2012, pp. 121 - 126.

[4] S. Cheung, M. Fong, P. Porras, K. Skinner, and V. Yegneswaran, "Securing the Software-Defined Network Control Layer," 2015.

[5] Ferguson AD, Guha A, Liang C, Fonseca R, Krishnamurthi S. Participatory networking: An API for application control of SDNs. In: Proc. of the ACM SIGCOMM 2013 Conf. on SIGCOMM. Hong Kong: ACM, 2013. 327 – 338.

[6] Shin S, Song Y, Lee T, Lee S, Chung J, Porras P, Yegneswaran V, Noh J, Kang BB. Rosemary: A robust, secure, and high-performance network operating system. In: Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security. Scottsdale: ACM, 2014. 78 – 89.

[7] WU Jiang-xing. Study on Network Space Mimicry Defense [J]. Journal of Information Security, 2016, 1 (04): 1 - 10.

[8] Jajodia, S., et al., Moving Target Defense. 2011: Springer New York. 99 – 108.

[9] L. Lamport and M. Fischer, "Byzantine Generals and Transaction Commit Protocols," Computer Science Laboratory Sri International Op, 1982.

[10] Macfarland D C, Shue C A. The SDN shuffle: creating a moving-target defense using host-based software-defined networking [C] / Proc of ACM Workshop on Moving Target Defense. New York: ACM Press, 2015: 37 - 41.