Advances in Engineering Research (AER), volume 148
3rd Workshop on Advanced Research and Technology in Industry Applications (WARTIA 2017)

Research on the Vulnerability of Software Defined Network

Binbin Lin*, Xueyong Zhu and Zhiguo Ding
Network Center, Electronic Engineering Instutite, Hefei AnHui, China
Binne_LinBB@163.com

Keywords: SDN, Vulnerability, Determining, Model

Abstract: With the continuous evolution of network technology, Software Defined Network (SDN) has become technical trends to solve the existing network problems. SDN is a new architecture of network. It decouples data plane and control plane, and simplifies network management. The same time, its vulnerability is also a crucial issue to its application due to openness and programmable. This paper deeply analyzed the vulnerability of SDN in control plane and application plane. Then the model of evaluating SDN's vulnerability is presented. With this model we got a security framework of SDN. Finally, we preliminary analyzed how to reduce the vulnerability of SDN.

1. Introduction

Software Defined Network (SDN) is an inevitable development direction of the next generation network. However, SDN still has many problems. Its security has been greatly affected due to openness and programmable. Openness and programmable also make SDN become vulnerability. Therefore, it is necessary to research the security problem of SDN and find the theory and method to enhance the security of SDN. November 4, 2012, the Internet Engineering Task Force (SAAG Advisory Group) released the security requirements in the SDN architecture, mainly discussed the security requirements between the SDN control and the application plane, including security issues such as the security interface between the control and application plane, authentication, authorization, application, and visibility of security policies between embedded applications. But it did not provide a solution to remove the security threats in SDN. From literature we can see that the research of SDN is mostly about how to application it. The security research of SDN is rare[1].

At present, SDN is mostly based on OpenFlow protocol and its security and vulnerability research is still in initial level. This paper mainly research SDN based on OpenFlow protocol. We analyzed its vulnerability in the control plane and the application plane, and established the decision model of vulnerability. Then we constructed a protection control architecture of SDN.

2. Technical Architecture of SDN

SDN controller is the core of network control. The programmable of network and network application are realized through standardization. Technical architecture of SDN is shown in Figure 1.

In this architecture, network defined by software. Network administrator implement more flexible network controls without manually changing the configuration of each network device.

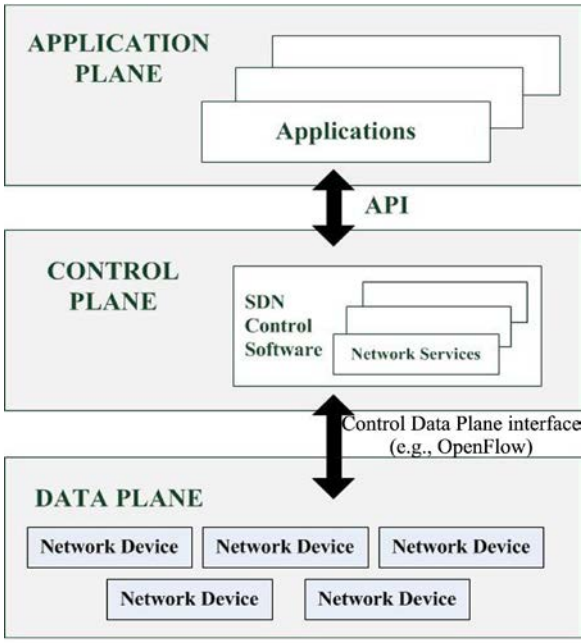

Figure 1 Technical framework of SDN

SDN controller monitors the state of network infrastructure, so administrator can deploy network resources more intelligently and flexibly. In application plane, user can formulate network application strategy which conforms to its business requirement through the standard north-facing interface to realize the flexible scheduling of network resources. At present, the implementation of SDN network is mostly based on OpenFlow protocol[2]. The latest OpenFlow protocol is released in October 2013 named version 1.4. OpenFlow technical architecture is shown in Figure 2 [3]. Specific control policies are represented by flow tables and table entries. Each flow table consists of fields such as match field, counter, instruction and so on.

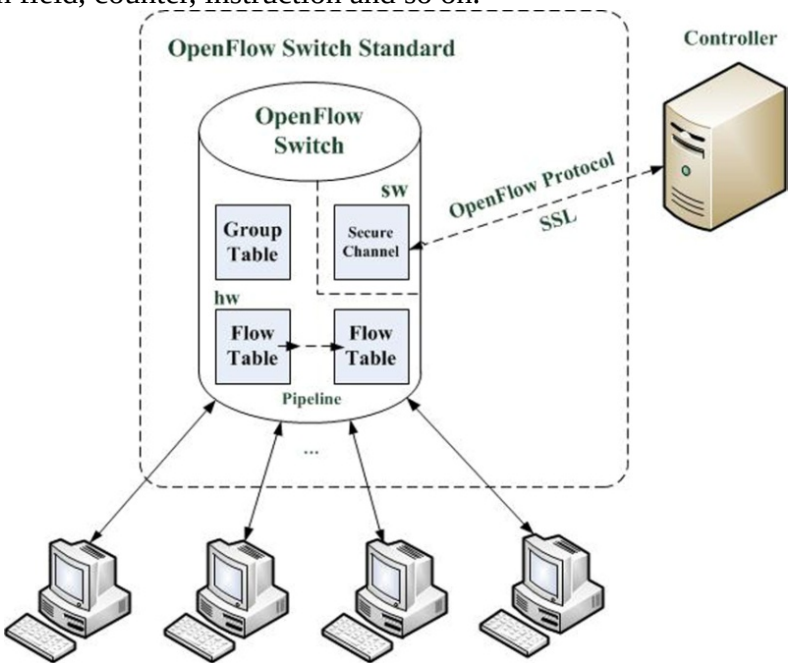

Figure 2 Technical framework of OpenFlow

In flow table, we can match any field according to the network grouping in the network packet header, such as L2, L3, L4 layer. In addition, OpenFlow management and configuration protocol manages data flow configuration in OpenFlow switch to ensure the smooth transmission of the data stream between the SDN controller and the OpenFlow switch.

3. Safety Characteristics of SDN

The security technology architecture of SDN put forward safety evaluation system and safety management through data plane, application plane and control plane. SDN also developed a series of safety evaluation standards to evaluate and grade network equipment, services and applications. Some applications or service, which have low security level, will be messaged to the controller, then the controller perform corresponding procedure. Its security management provides differentiated security policy configuration and management for different managers through a visual control interface. However, because of the programmability and open of SDN network, the security evaluation and management are not easy to realize. So the security of SDN network still has many problems. In fact, SDN architecture brings the flexibility of management, operation and application, and also generates some unique security problems[4].

SDN controller centralized network configuration, network service access control, network security service deployment and so on. An attacker who successfully implemented an attack on a controller would result in a large area of network service paralysis. Under SDN architecture, attackers ' attacking objects are concentrated. And the attack difficulty is greatly reduced.

Openness is another important feature of SDN, which can realize unified management, configure heterogeneous network devices and provide programmable ablity. But openness also makes SDN face more security threats.

First of all, openness makes security bug of SDN controller and incomplete strategy fully exposed to the attacker and gives attacker enough information to make relevant attack strategy.

Secondly, SDN architecture provides a large number of programmable interfaces to application plane through SDN controller. This level of openness may lead to misuse of interfaces, such as triggering DDoS attacks.

4. Vulnerability of SDN

From above analysis, SDN’s vulnerability problem is mainly concentrated in control plane and application plane.

4.1. Vulnerability of the Control Plane

Centralized control plane is the backbone of network service, which is directly related to the availability, reliability and data security of network services. Compared with traditional network, SDN controller is an important vulnerable point, which is the first problem to be solved in SDN security. In control plane, the threats facing the control plane are as follows[7]:

1) Network monitoring

Network attacker obtains the controller’s cut-in point from the network, and then forges and modifies control signal.

2) IP address spoofing

Network attacker forges IP address to mock IP address through network monitoring to get trust of the switch or router. Network equipment can be manipulated to do whatever network attacker wants to do.

3) DDoS attack

The attacker sends multiple service requests to the controller, and all the requested return addresses are forged, which can overload the controller and refuse service.

4) Virus, worm and Trojan attack

The attacker gets control of the controller and embedded malicious code through loopholes existing in the controller.

Definition 1 Vulnerability of SDN control plane

For a normal operation of SDN network system, if the attacker can manage or dispatch system resources (such as exchange, routing, access control, flow control, throughput control, etc.), and make the function or performance of SDN system affected, it is said that SDN control system is fragile, that means SDN control plane is vulnerable.

Formal Description:

Set the attacker is A. Control signal (or system resources) is Sc and $f()$ is the control function of attacker A (such as forgery, deception, control, transformation, etc.). D_A is an attack target. Then the vulnerability of the control plane can be described as: If A gets or controls Sc, there will have a control function $f()$, which makes the $D_A = f(Sc)$, then A 's attack is successful. This time SDN control plane is vulnerable.

Obviously, the complexity of $f()$ determines the degree of vulnerability of SDN control plane. Usually we have to design a good control plane signal structure and control transmission strategy using secure transport protocol to make $f()$ become a difficult function. At this time, A need very sophisticated skills to achieve a successful D_A. So the attack difficulty greatly increased. The vulnerability of SDN control plane is significantly reduced.

At present, OpenFlow protocol and SSL protocol are used to communicate between SDN controller and general network devices. And the vulnerabilities of those two protocols are also the source of SDN control plane's vulnerability. It is important to design a control transport strategy based on these two protocols.

Definition 2 Controlled vulnerability of SDN control plane

A normal operation of SDN network system, if it is a resource strategy of the management and dispatch system to counter attack, so that the function and performance of SDN network system can be played normally, the vulnerability of the SDN control system is controllable. That means the network owner has the strategy to control the vulnerability of SDN control plane.

Formal Description: Set P is a set. P means all control transmission policy of SDN controller. p is the control of the transmission strategy, $p \in P$. g is the control strategy application function. If $Pc = g(p)$, is to enable the normal operation of SDN control strategy set, and $Se(a(i))$, make $f(Sc) \neq D_A$. Then SDN Network control plane vulnerability is controllable.

In order to evaluate controllability, the weak controllability of SDN network control plane can be simply expressed as follows:

$C_{SDN} = |Pc| / |P|$, $|P|$ is the number of control strategies that apply function g to control vulnerabilities by controlling the strategy $|P|$ is the number of total control policies owned by the controller.

For example, set the

$$p = \left\{ \begin{array}{l} binding\ switch\ device\ MAC,\ binding\ the\ controller\ MAC, \\ restrict\ the\ forwarding\ destination\ MAC\ Address\ table, \\ restrict\ the\ forwarding\ source\ MAC\ Address\ table, \\ set\ IP\ ACL,\ restrict\ source\ IP,\ set\ port\ ACL, \\ control\ instruction\ check,\ limit\ OpenFlow\ channel, \\ set\ the\ ACL\ of\ flow\ table,\ Set\ port\ count, \\ restrict\ controller\ domain\ scope \end{array} \right\}$$

Then, for the forwarding function of the package, the function g can be $Pc = p$ by designing the appropriate control policy, and for the forwarding function, $C_{SDN} = 1$, the transmission control strategy P is fully controllable for the packet forwarding function.

And for the routing function, by designing the appropriate control strategy to apply function g, make

$$pc = \left\{ \begin{array}{l} binding\ controller\ mac,\ set\ IP\ ACL,\ restrict\ source\ IP, \\ set\ port\ ACL,\ control\ instruction\ check, \\ restrict\ OpenFlow\ channel,\ set\ the\ ACL\ of\ flow\ table, \\ set\ port\ count, limit\ controller\ domain\ scope \end{array} \right\}.$$

Then $C_{SDN} = |Pc| / |P| = 9/12 = 0.75$. These transmission control strategies P routing is 75%

controllable. Of course, this is related to the control strategy of the controller applying function g, and the number of total control strategies owned by the controller must be large enough.

In this way, the vulnerable controllability of SDN network control plane becomes the search for good control strategy application function g and the largest C_{SDN} make it close to 1. That is, under this controllability definition, our vulnerability management goal is to find the appropriate control strategy P and control strategy application function g, make $|Pc|$ as large as possible, nearer $|P|$ the better, the best case is $|Pc|=|P|$. The constraint is that the total number of control policies owned by the controller must be large enough.

Obviously, the control strategy of the design control plane p and its application function g is very important. A good function g will make the Pc maximum, and it also increases the complexity of the attack function f. Both the function f and g are affected by the API interface and signaling structure of the programmable function of the controller and the mode of transmission.

Usually, the control strategy of the design control plane and its application function g must consider the impact of the attacker function f. Those two functions have a certain dependence, so the actual use of both the attacker's function f, but also to study the control strategy application function g. If you can find dependencies between the corresponding function f and the function g for a control strategy p, it is good for us to control the vulnerability of the SDN network control plane.

4.2. Vulnerability of the Application Plane

The application layer will provide a variety of complex network application services through application programming and management strategy, and it also has the same vulnerability problem because of the programmability of the application level. The vulnerability of the application plane mainly includes:

1) Malicious application: Through the application layer of the application of worms, spyware and so on, to steal network information, change network configuration, occupy network resources and so on, so as to interfere with the normal working process of the control plane, so that the controller control of the network confusion.

2) Application of the Security rule conflict: In order to provide various types of network application services, the application layer needs to develop security rules to access some of the controller's security interfaces. With the complication of application, there is a conflict of security rules between multiple applications, which leads to the confusion of network services and the increase of management complexity.

In order to reduce the vulnerability of SDN application plane, it is necessary to consider the manageability of SDN application. Only SDN application is manageable, and the vulnerability of its application plane can be controlled.

Definition 3 Vulnerability manageability of SDN application plane

For SDN network application service system, if the strategy of managing and dispatching system resources exists, the application service system of SDN application plane will has different safe running performance. It is said that the vulnerability of SDN network application plane can be managed by the control strategy.

The formal description is: Set $Pm=\{a(i)\}$. It is a collection of control policies that enable SDN to apply the service target T safe operation. $Se(a(i))$ indicates the security performance of SDN application services under control strategy $a(i)\in Pm$ for SDN application plane service. If there is a mapping function $M:Se\to Se$, as well as different strategies $a(i)$ and $a(j)\in Pm$, can make $Se(a(i))\neq Se(a(j))$, then M is called SDN application management of network application. At this time the application service target T of SDN network application plane is to be managed

under control strategy $a(i)$ or $a(j)$ application service frangibility.

When SDN applications are managed in accordance with the vulnerability of strategy $a(i)$ or $a(j)$, the vulnerability of the SDN network application plane is controlled. Of course, for different $a(i)$ or $a(j)$, the performance of the SDN application service may be different, but it can provide application services to a certain extent, even if the service is not very good.

Application management mapping M is usually selected as follows: if $Se(a(i)) > Se(a(j))$, then M choose application control strategy $a(i)$. If $Se(a(i)) < Se(a(j))$, then M choose application control strategy $a(j)$ until a better application of the control strategy is selected to minimize the vulnerability of SDN application plane. And at this time, SDN network application service performance also achieves better or best.

Based on this definition, application service performance for a given SDN network application plane, such as availability, confidentiality, integrity, reliability, service type, service port, application type, API interface rule requirements, and so on, can be evaluated using the security performance $Se(a(i))$ under the application of control policy $a(i)$. In this way, the vulnerability of the SDN network application plane becomes a problem of finding $a(i)$ to maximize $Se(a(i))$ so that the vulnerability of the SDN network application level is minimized and the service performance is best. The search for:

$$S = \underset{a(i) \in Pm}{Max}\ Se(a(i))$$

5. Discussion on Reducing the Vulnerability of SDN

To build a secure SDN network, reduce the vulnerability of SDN network, it is necessary to effectively manage the equipment, application, security control strategy, instruction transmission strategy, application service management strategy and performance. We discuss the vulnerability of SDN from the control plane and the application plane. Based on the analysis in the previous section, we build a protection control strategy of SDN network. As shown in Figure 3.

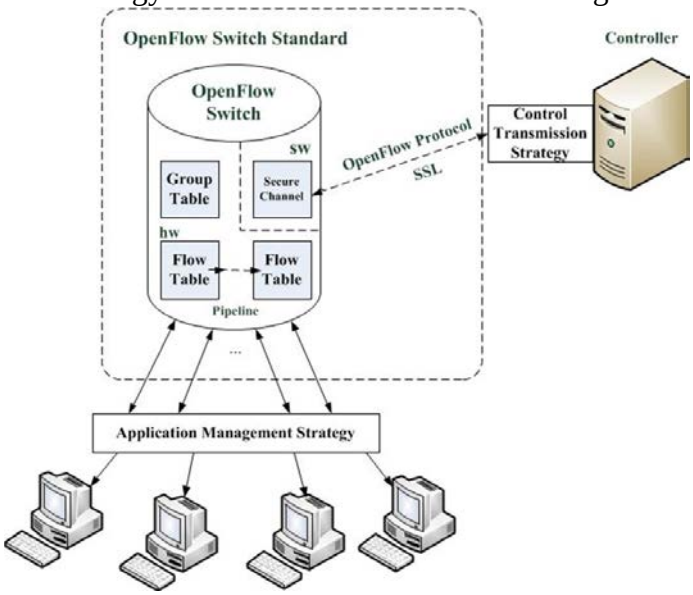

Figure. 3 Protection control strategy architecture of SDN network

The first is to increase the control of the transmission strategy in the control level. The controller's transmission control and access control is fragile controllable and manageable, and does not allow the controller API programming interface to be too open and make it under the security rules, and control the instruction transmission. The second is to increase the application management strategy in the application level. The Open service, application service access rules and the programmable interface of application are managed and controlled. [5]

At the control level, the security policy control is configured and managed by the controller. And the exchange, routing and forwarding are carried out through the control instructions issued by the controller. So the control of the control plane increased the transmission strategy. The controller has a series of strict authorization, access control, security management, programming interface control and other rules. So that the perceived abnormal network equipment, abnormal behavior in time to isolate, to avoid large-scale damage. At the same time the controller according to the control transmission strategy can analyze the network behavior ability according the log, the traffic, the current service and so on.

It is usually required that the control level must be designed with a sufficient number of control strategies p and its application function g, so that the controller obtains enough effective control strategy to $Pc \subset P$ the number of $f(Sc) \neq D_A$. And the design of the control strategy application function g relative to the attacker's function f must be complex enough. This minimizes the vulnerability of the SDN network control layer to ensure the safety of the control plane of the SDN network.

At the application plane, using the increased application management strategy, the application plane has a series of security service access rules and application management strategy, can be used to provide services, as well as the need for the interface of the controller to identify, the application of rules and policies to be allowed to become a legitimate application in SDN. It can also be used to monitor and eliminate security threats with the management control strategy of programmable interface and the existing technology, and further strengthen the security protection of the application plane controller[6]. At the same time, the application plane has access control strategy, which can prevent attackers from using the open interface to attack the network controller through the application service, and use some interfaces to monitor the network.

Usually for each application plane, an application management strategy must be found $a(i)$ to make the $Se(a(i))$ the largest, so that the vulnerability of the SDN network application plane is minimized and the service performance is best applied to ensure the security and reliability of the SDN network application service.

6. CONCLUSIONS

At present, the research on the security and vulnerability of SDN network is still in its infancy. This paper first analyzed the SDN technical architecture principle and the development present situation. We researched the security characteristic and the vulnerability question in the SDN structure, analyzed its vulnerability in the control level and the application level and proposed the corresponding vulnerability question judgment model. On this basis, the architecture of the protection control architecture is constructed. This architecture explore controllable and manageable problems of network, which is expected to promote the further research on the security and vulnerability of SDN network.

REFERENCES

[1] Software-Defined Networking: The New Norm for Networks, ONF White Paper, April 13, 2012, Open Networking Foundation.

[2] OpenFlow Switch Specification Version 1.4.0 (Wire Protocol 0x05), October 14, 2013, Open Networking Foundation.

[3] OpenFlow switch specification, version 1.1.0. http: //www.openflow.org.

[4] D, Kreutz et al., "Software-Defined Networking: A Comprehensive Survey", Proc. IEEE, vol. 103, vol. 1, pp. 14-76.

[5] G.Papageorgiou, J.Gasparis, S.V. Krishnamurthy, R. Govindan, and T. La Porta. Resource thrifty secure mobile video transfers on open wifi networks. In Proceedings of the Ninth ACM Conference

on Emerging Networking Experiments and Technologies, CoNEXT ’13. ACM, 2013.

[6] T. Kohno, A. Broido, and k. claffy. Remote physical device fingerprinting. IEEE Transactions on Dependable and Secure Computing, 2(2):93–108, May 2005.

[7] Hoque N, Bhuyan M H, Baishya R C,et al. Network attacks: taxonomy，tools and systems. Journal of Network and Computer Applications, 2014, 40: 307-324.