Research on SDN Flow Secure Access Control

Hu Yang and Lei JiaXing
Computer Department, Guangzhou Civil Aviation College, Guangzhou 510470, China
huyangfox@163.com

Abstract. In order to ensure the Software Defined Network (SDN) flow security access, this paper puts forward a SDN terminal access control system through the deep study on the terminal security access solution in the existing SDN. This system combines the traditional terminal access control technology with the new SDN network and mainly implements some functions such as user's identity authentication, terminal security status assessment, user's service authorization, QoS control, and so on. Simultaneously, the system security is analyzed in detail. The network simulation in Mininet is carried out in combination with the RYU controller secondary developed so as to complete the experiment of access control function and communication delay performance. The results show that the security access control system of SDN flow has flexible access control security strategies and then can detect the threats from the insecure terminal access in SDN. This can not only realize the identity authentication of users but also ensure the security of access terminal, and thus realizing the access authorization of terminals in different safe states.

1. Introduction
The SDN, proposed by CLean State research group of Stanford University, is an implementation way of network virtualization. Its core principle is that the traditional network system is decoupled into three planes of control, data and application by OpenFlow protocol, the forwarding path is calculated for the specific business data flows to generate the flow table, and then some control informations, such as safe service, network configuration, etc., are translated into the network data and then reported to the controller by physical switches, some network equipments, forwarding equipments and the OpenFlow protocol [1]. Until now, many well-known enterprises at home and abroad, such as NEC, Cisco, Ali, Huawei, etc. have carried out in-depth research on SDN.
2. Related work

SDN, driven by the development of cloud computing, is widely used, however, the new threats for the network security also appear in the new network architecture of SDN. For example, the security threats of SDN mentioned in the literatures [2-6] include malicious scanning, unauthorized access, and denial of service attacks, among them, the malicious scanning is a preparation for the unauthorized access and denial of service attacks, moreover, the unauthorized access and denial of service attacks would result in the network damage, thus limiting the extensive promotion and deployment of SDN.

But due to the complexity of the algorithm, there exists a larger delay, so the promotion and application effects are poor. With the extension of the business of cloud computing, the number of users of network access is growing, and the network application environment is more and more complex. Until now, the reasons for the security problems are as follows. On the one hand, the virus library access to the terminal platform has not been updated, as well as the operating system lacks the patches. This would make the threats, such as network Trojan, ransomware, and so on, intrude into the network and arbitrarily spread, thus causing huge damage. On the other hand, a large number of server resources are consumed, which is caused by distributed denial of service attacks (DDoS), etc., and finally, resulting in the server crash.

Therefore, for the network security of SDN, it is an import problem to be solved that how to establish a network access security mechanism in order to effectively prevent the malicious scanning of illegal users and the network attack behavior of "legitimate users" by the terminals that do not conform to the safe strategies.

3. FlowSAC system

3.1. FlowSAC system establishment

Based on the findings mentioned above, this paper proposes a Flow Security Access Control (FlowSAC) system based on OpenFlow in combination with the potential safety hazard of SDN network. In this system, the user access mechanism combines with the terminal security assessment, a two-layer security mechanism is set. Firstly, the legal detection is conducted on the users, then, after the terminals for users access connect the network, the SDN terminal is evaluated to ensure that the access terminal is safe and reliable.

The FlowSAC system structure is shown in Figure 1, mainly including OpenFlow switch, controller, authentication and security state assessment server (ASA) and security server area. The OpenFlow switch communicates with the controller through the OpenFlow protocol, and the network data are transmitted according to the flow table from the controller. The controller is the control center of the whole network, which is responsible for access control and authorization, exchange path calculation, flow table generation, distribution, deletion, etc. The controller masters the whole network view and can dynamically generate the data forwarding flow table, so the FlowSAC system can realize flexible access control and authorization based on data flow. The ASA is responsible for specific user identity authentication and security assessment of access terminals. Moreover, the specific authentication way and security assessment policies can be specified and dispatched by the controller. Furthermore, the SDN has flexibly programmable characteristics, the users can easily deploy multiple authentication ways through the interface provided by the controller and update the security assessment policy.
according to the network security requirements. Some safe services for access terminals are mainly provided in the security server area, such as the patches for the operating system, virus library update, and so on. And the functions can be extended according to the actual needs of network security. FlowSAC system has six states, namely, the initial state, user authentication state, terminal security evaluation state, isolation repair state, state to be authorized and access authorization resource state, as shown in Figure 2.

3.2 Work principle of FlowSAC system
The work process of FlowSAC system mainly includes identity authentication, terminal security evaluation and authorized access. The identity authentication process supports multiple authentication ways, as well as the terminal security evaluation process can support the self-defined security evaluation policy. Moreover, the authorization access process can make the user identity information mapped to a specific combination of MAC and IP addresses, thus realizing the authorization based on OpenFlow data flow. The specific work process is as follows.

1) The user sends an network access request to the OpenFlow switch, and then the OpenFlow switch sends the access request to the controller in a way of packet-in. The controller checks whether the MAC and IP addresses of the terminal are in the network access scope allowed by the access control list ACL, and if the access network is allowed, the identity authentication request is sent to the user.

2) The controller generates two flow tables for users. One flow table path is from OpenFlow switch A, OpenFlow switch C to ASA (A->C->ASA), and the other one is from OpenFlow switch A, OpenFlow switch D to the safe server area (A->D-> safe server area), as well as it forwards two flow tables to each OpenFlow switch. Furthermore, the OpenFlow switch can only forward the authentication data flow, failing in forwarding the business data flow of users.

3) If the MAC address or IP address of the terminal is in the list forbidding access network of ACL, the controller would send a prompt message that the terminal has no permission to access the network to the OpenFlow switch, and the prompt message would be forwarded to the user by the OpenFlow switch.

4) If the identity authentication of users passes, ASA would send the security state evaluation requirements of the terminal platform to the users and simultaneously forward the safe evaluation strategy. The terminal detects the operating system version, virus library, open port, software
installation and so on according to the safe evaluation strategy, and then the safe state detection results are reported to the ASA.

5) ASA analyzes the safe state detection results from the terminal, if not conforming to the safe strategy, the terminal is required to update the safe state, and then the terminal would be in the isolation repair state and then visit the safe server area for corresponding security repair, finally, the safe state information of terminal after repair would be reported to ASA.

6) If the security state detection results reported from the terminal conform to the safe strategy requirements, the user ID, which has passed the identity authentication, and the safe state evaluation results of terminal are fed back to the controller by ASA, and then the controller would set the terminal in a state to be authorized. Thus the user completes the network access, but it is still unavailable for the access to the specific network resources.

7) The user sends the first business packet for access to the specific network resources to the OpenFlow switch. Since there is no business flow table available for the OpenFlow switch at this time, the OpenFlow switch sends the business packets to the controller in a way of packet-in.

8) The controller looks up the user's ID corresponding to the MAC address and IP address in the business packets and then authorizes them according to the resource authorization list. If the user's ID is in the authorization list of network resources to be visited, the controller generates the business data flow tables for the user (A>B>application server) and sends the flow tables to each OpenFlow switch, then the user can visit the specific network resources. However, if the user's ID is not in the authorization list of network resources to be visited, the controller would not generate the business flow tables, and the terminal is still in the state to be authorized. After the authorization for users is successful, in order to avoid the excessively large load of safe equipments, this paper adds the LimitAPP and QoSAPP modules in the RYU controller to ensure the security of simultaneous access to the network for a large number of users with the functions selected by QoS paths and different communication paths assigned according to the user level. LimitAPP module has two functions, namely, 1) One function is to make the network architecture information of OpenFlow switch stored in the SQL database for the use by QoSAPP. 2) The other one is to monitor whether the network architecture of OpenFlow switch changes in real time and then immediately inform QoSAPP of this change. The information stored in the database includes OVS network architecture, source MAC address, destination MAC address, physical port of source and physical port of destination of OpenFlow switch, the roles and permissions of users, as well as the bandwidth required from source to destination.

4. Experiment and results analysis

4.1 Experiment environment

In this paper, the experiments are carried out in a lightweight SDN simulation platform Mininet supporting the OpenFlow1.3 protocol. The open-source RYU controller and the OpenFlow switch software OpenvSwitch2.0.2 are used. In addition, the application server supports E-mail, FTP, TELNET, HTTP, and so on, as well as ASA and safe server area are set on PC (patch server and virus library server). Moreover, the 64-bit Win 7 operating system, Corei5-3470 CPU, 3.2 Ghz main frequency and 4Gb memory are adopted for all PCs in experiments so as to run FlowSAC system. The 64-bit
Ubuntu14.04LTS is installed in the virtual machine VMvare, the RYU controller is installed in the Ubuntu system, and then the Python2.7 is used for the secondary development. The network simulation topology, built by Mininet, is connected with the self-defined RYU controller. Four OpenFlow switches are connected with ASA, security server area (patch server, virus library server), application server and user, respectively.

4.2 Access control function experiment

The first experiment evaluates the efficiency of the FlowSAC system discarding unauthorized user data packets (see Figure 3). In this paper, the iperf network performance testing tool is used for testing. The client sends the UDP packets by a self-defined output tool at a constant rate of 30 Mbps. Packets would not reach the application server because they don’t pass the authentication. It takes 25s for FlowSAC system to conduct the identity authentication and platform security state evaluation, the data packet of business can be sent to the application server after a 2-3s delay. The reason for delay is that the controller authorizes the user's ID according to the resource list to generate the business data flow tables, and then they are sent to the OpenFlow switch. Experimental results show that packet can only be forwarded after the identity authentication and security platform security state evaluation, otherwise, the packet would be discarded.

The second experiment evaluates the validity of FlowSAC system as the revocation of authentication. In this paper, the iperf network performance testing tool is used for testing, and the experimental results are shown in Figure 4. For the communication between the user and the application server, assuming that the users has passed the identity authentication, however, the identity authentication is revoked after 15s, the users can’t continue to visit the application server. It is observed from the experiment that the delay to block the network traffic of the application server is 1.5s. The reason for the delay is that the controller sends orders to the OpenFlow switch to delete all the flow tables of the user terminal. After 24s, the user authentication is restored, and the delay for authentication recovery is about 2.5s. Thus, the experimental results in this paper show that the FlowSAC system is effective in releasing or blocking the flow by forwarding or discarding the packet.
During the process of experiment, the user terminal platform state is the same, as well as the same IP address and MAC address. The only difference for each test scene is the ID of the requester. The experimental results suggest that the user can only visit the network service combination corresponding to the ID.

4.3 Communication delay

The performance of FlowSAC system and the access delay index can be evaluated by time delay test.

1) Comparison of ICMP response time under different conditions

In the experiment, the FlowSAC system is compared with common OpenFlow controller and the ping time of conventional network. Furthermore, the ping time refers to the period from ICMP request message to the ICMP response message. When the first ping is received, the OpenFlow controller performs the authentication, but as receiving the ping for more than two times, the OpenFlow controller does nothing, because the flow table information of OpenFlow switch has been written in the forwarding column at the first ping. Therefore, the time for the first ping and the second ping is evaluated, respectively.

Two results can be obtained from the first ping time, namely, (1) the basic function processing time of the OpenFlow controller is 10.1 ms, (2) the processing time of OF-TAC system resource list authorization is 9.5 ms. From the second ping, the forwarding rate of packet is almost the same as that of the regular network without any operation of OpenFlow controller.

2) Time of identity authentication and platform security evaluation

The time of identity authentication and platform security evaluation is tested in the experiments. Among them, the time of identity authentication refers to the period from the users’ request access to the network to the successful identity authentication. Furthermore, the platform security evaluation time is from the moment that ASA sends the terminal security platform evaluation requirements to users to the moment that the safe state information after repair returns to ASA. In order to obtain the accurate results, the performance of each datum is tested for five times. If the number of users increases, as expected, the authentication time accordingly increases. The identity authentication time of users would also increase with the increase of load, but compared with the increase in authentication time caused by the increase of the number of users, the increase of authentication time is acceptable. Hence, the FlowSAC system would be rapidly responded if applied in the actual service communication. Because the safe states of clients are different, the security evaluation time of platform is greatly different. Furthermore, the connected client after the isolation repair of the first platform security evaluation has already been in a safe state, and the time for the second platform evaluation approximately equals to the basic processing time for the platform evaluation.

3) Key information processing delay of packet header

In order to analyze the time needed by key information processing (source/destination address and access control check function) of packet header as the identity authentication of users in the FlowSAC system in detail, this paper carries out the tests for the data header information extraction and processing time as single user authentication, and the results are shown in Figure 5.
5. Conclusions

The security of SDN access control is mainly to establish fine-grained access control mechanism to prevent illegal users and terminal platforms which do not meet the requirements of security strategy from connecting SDN. With the wide use of SDN, it is significantly important to ensure the security of SDN. The network architecture with a separation between SDN control and forwarding planes can realize the centralized control by the controller, which provides a guarantee for the network security.

The FlowSAC system proposed in this paper is a SDN terminal access control mechanism in which the identity authentication of users combines with the terminal security state evaluation. On the one hand, this mechanism can prevent the malicious terminal access network which would result in denial of service attacks by identity authentication. On the other hand, the terminal platform security state evaluation and repair can prevent the spread of ransomware and Trojans. The evaluation strategy for the terminal security platform in FlowSAC system is still relatively simple, until now, only including the patch for the operating system and update for the virus library, as well as it would be expanded according to the actual needs of network security in future.

6. References

[1] ZHANG Chaokun, CUI Yong, TANG Heyi, et al. State-of-the-Art Survey on Software-defined Networking (SDN)[J]. Journal of Software, 2015, 26(1): 62-81.

[2] BENTON K, CAMP L J, SMALL C. Open Flow Vulnerability Assessment[C]//ACM. 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, August 16, 2013, Hong Kong, China. New York: ACM, 2013: 151-152.

[3] KULIESIUSF, DANGOVASV. SDN Enhanced Campus Network Authentication and Access Control System[C]//IEEE. 8th International Conference on Ubiquitous and Future Networks, July 5—8, 2016, Vienna, Austria. New jersey: IEEE, 2016: 894—899.

[4] DANGOVAS V, KULIESIUS F. SDN-Driven Authentication and Access Control System [EB/OL]. https://www.researchgate.net/publication/263917691_SDN—Driven_Authentication_and_Access_Control_System, 2017—12—23.

[5] LOU Hengyue, DOU Jun. Research on DoS Attacks Against Control Level in Open Flow-based SDN [J]. Computer Science, 2015, 42(11A): 341-344.
[6] ZUO Qingyun, ZHANG Haisu. Analysis and Research on Network Security for Open Flow-based SDN[J]. Netinfo Security, 2015(2): 26-32.

Acknowledgments

This work is partially supported by Natural Science Foundation in University of Guangdong (No.GDJS2019303)