A Study of SDN Security Problems

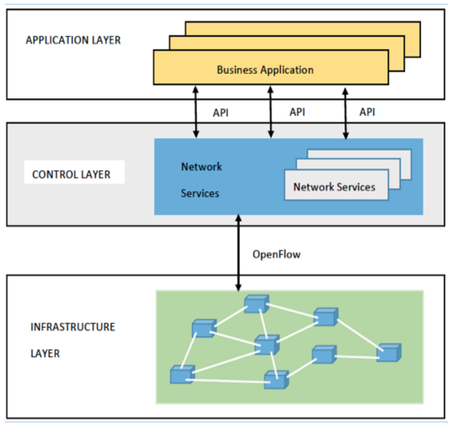
Mengqi Wang, Lening Wang

Department of Electrical Engineering, San Jose State University

Introduction

The Internet has become a basic but important facility nowadays. However, the more Internet technologies are used, the more problems can be identified. In order to provide a better quality of service and to enhance the scalability and flexibility of modern networks, Software Defined Networking (SDN) has been proposed. SDN technology and OpenFlow protocol have gained a lot of attention and been recognized in academic area as well as industry in recent years.

SDN has its own characteristics such as the centralized mode, the OpenFlow switch, etc. An SDN network is divided into three layers, the application layer, the control layer and the infrastructure layer. External structures of these layers are independent. However, internal structures are connected with each other.



SDN is a brand new concept, which also presents many problems. Our project aims to explore potential network security problems of the SDN architecture and enhance the SDN network safety performance. We simulated two secure problems in the SDN network, and found effective defense methods.

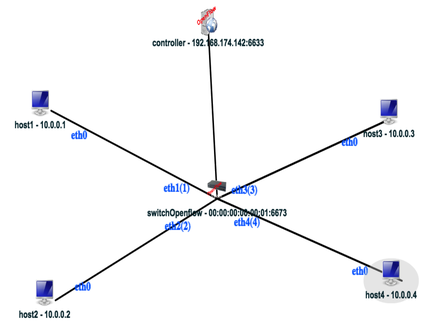
1. DoS Attack
- DoS Attack in SDN hosts
- DoS Attack to the SDN controller

2. Illegal Access
- Illegal Access between SDN hosts
- Illegal Access to the SDN controller

Based on data analysis, a defense mechanism was proposed and implemented. The strength and weakness in SDN security were identified as well.

Methodology

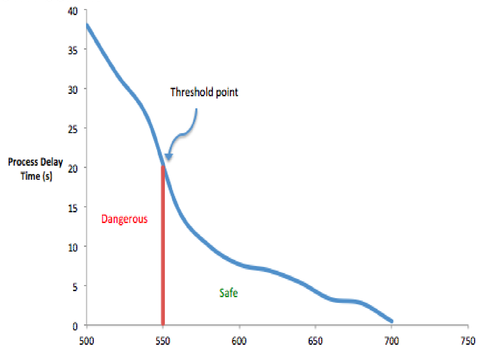
Mininet is used to build an SDN simulated network. The topology shows below.



- One Central Controller cO
- One OpenFlow Switch s1
- Four hosts: h1, h2, h3, h4

DoS Attack in SDN Hosts

This DoS attack happens inside the SDN network. H1 is selected as the hacker, an HTTP server run on h3 as the victim. After modified the time interval between two continuous SYN flows sending from h1 to h3, the result is shown below.



1) With the increase of the time interval, the process delay time would decrease
2) When the time interval is less than 550us, this HTTP server stopps working

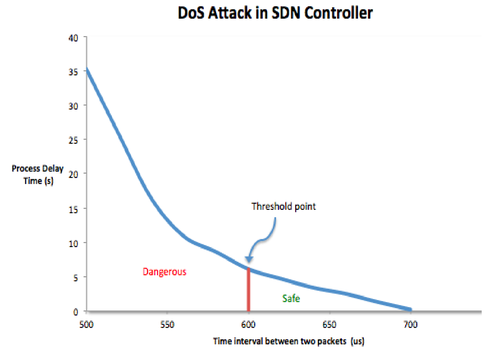
DoS Defense in SDN Hosts

- Manually Stop DoS Attack in Controller

  Find out the attacker in the SDN central controller monitor, then disconnect the attacker or reduce the communication bandwidth of the attacker.

DoS Attack to the SDN controller

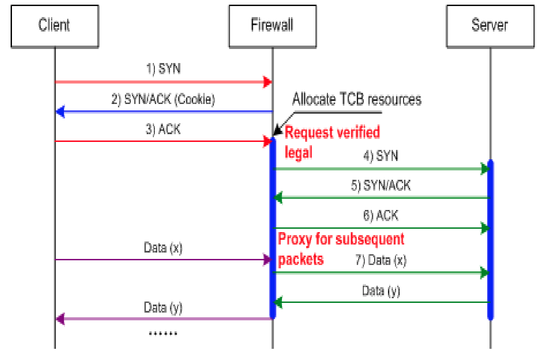
This DoS Attack happened outside the SDN network. H5 is pretended as the hacker , who located in a Kali Linux System outside this SDN network, to launch a DoS attack to the SDN controller. After modify the time interval between two continuous SYN flows sending from h5 to the controller, the result is shown below.



1) With the increase of the time interval, the process delay time would decrease
2) When the time interval is less than 600us, the controller stops being connected and the whole SDN network is disabled.

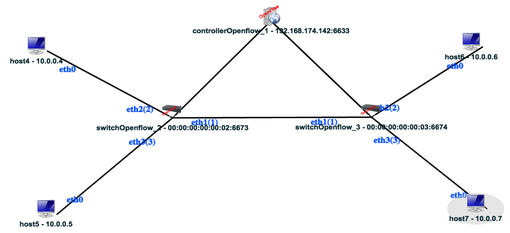
DoS Defense to the SDN Controller

- Firewall
- SYN cookies



Illegal Access between SDN Hosts

This illegal access happened between SDN hosts. One host under the SDN network illegal access to another host under the same SDN network. The topology is shown below.



Illegal Access Defense between SDN Hosts

- Set up limit access of each host
- Set up firewall for sensitive hosts
- Patch the SDN network

Illegal Access to the SDN controller

We discuss two possible methods which could launch a illegal access to the SDN controller.

1) Illegal access to the machine which the SDN central controller run on
2) Illegal access to the OpenFlow switch

Illegal Access Defense to the SDN controller

- Update the system
- Strong authentication method
- One-time password, fingerprints, Retina scanner

Conclusion

1. The SDN network improve the network security in some area, like DoS attack in SDN hosts, illegal access between SDN hosts, etc.
2. The centralized mode network makes the SDN controller sensitive
3. Make sure the controller has no weakness
4. Make an effective recovery mechanism

Group Member