Software Defined Networking Security

Praarthana Ramakrishnan
Department of Computer Science
Clemson University
praartr@g.clemson.edu

***Abstract*— Software Defined Networking (SDN) provides flexibility in programming the network and supports problem solving remotely by building software for enabling network management. However, the current SDN design suffers from serious security issues due to its design. In this paper, the SDN architecture is discussed along with various threat factors affecting it are discussed. Later, the various principles and solutions to secure Software Defined Networking are discussed.**

***Keywords*— Security Attack vectors; Network Operating Systems; Dependability; SDN**

I. Introduction

Although Software Defined Networking allows separation of data and control plane and thereby providing flexibility for new applications, it inflicts a serious network security issue. Since the control plane is centralized, it can be easily attacked and so entails various protection methodologies. The two main advantages of SDN are network programmability and centralized control logic. These are the major causes of the threats related to SDN.

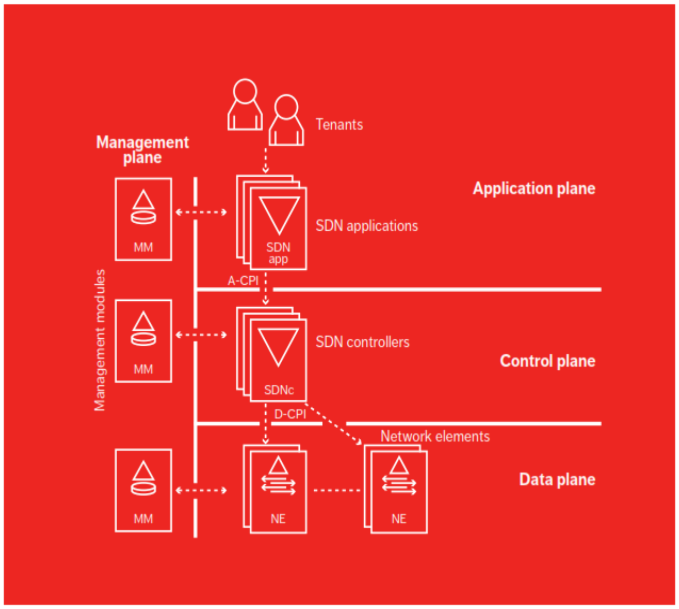

Fig 1. Architecture of SDN [3]

The Software Defined Networking Architecture is shown in Figure 1. To protect SDN against security breaches, it should follow the following principles:

i. Availability - Network must be functional even when there is a threat. In SDN architecture, the main component being the controller, if it fails to function, then it can lead to Denial of Service attack.

ii. Authentication and Authorization – Unauthorized access should not be allowed to access critical information. In SDN architecture, the network components should be secured from illegal access.

The possible threats at each layer of SDN are discussed below.

A. *Data Plane Attack*

The malicious users can gain unauthorized access and can attack the network elements, thereby causing Denial of Service (DoS) attack as shown in Figure 2. The implementation of user-friendly southbound APIs such as OpenFlow increases the network attacks. The attacker can divert the network traffic and try to sniff the packets and perform Man in the Middle attacks.

B. *Control Plane Attack*

Secondly, due to the centralization of the SDN control, it can suffer from single point of failure. Attackers can act as SDN controllers and break the whole network or cause cyber criminals. Centralized controllers are prone to vulnerabilities since they are built upon general computing platforms

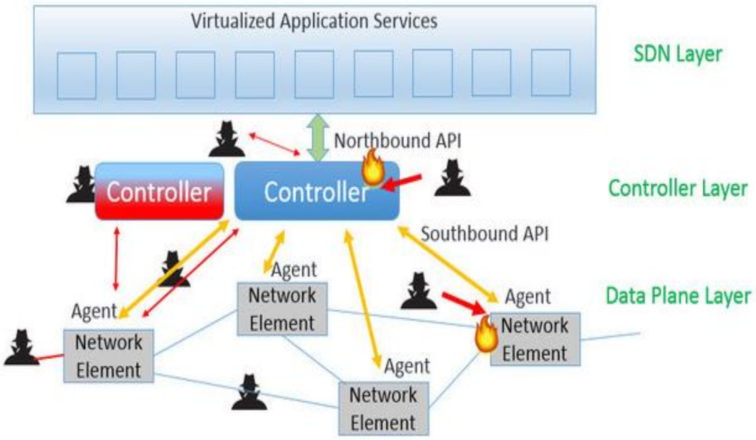

Fig 2. SDN Threats [1]

C. Application Layer Attack

Vulnerabilities in Application Programming Interfaces (API) such as Java are also possible. The attackers can hack the default password and analyze the packets and the SDN structure.

II. MAIN TECHNIQUES

The possible solutions in providing security to Software Defined Networking are discussed below in detail.

A. Data Layer Security Solutions

The Software Defined Networking uses Transport Level Security (TLS) for control plane security. But long sessions could make the data plane vulnerable to attacks. TLS can be used to authenticate between controllers and the SDN elements.

B. Controller Layer Security Solutions

Controller is the main component that severely affects the security of SDN. It needs to be observed for any doubtful activities by unauthorized users. For controller administrations, Role Based Access Control (RBAC) can be implemented, thereby securing the control plane. In order to avoid DoS attacks, the SDN architecture can use High Availability (HA) controllers instead of redundant controllers.

Keeping up-to-date records of CPU level, the memory utilized and statistics of the interface will help avoid threats. An extra layer of security needs to be applied to the sensitive data such as bank account information and personal details.

C. SDN Layer Security

For controlling traffic, Out-of-Band (OOB) network can be one of the possible security measure. OOB involves setting up trust boundaries to access network resources. [1]

D. Uniform Security Policy

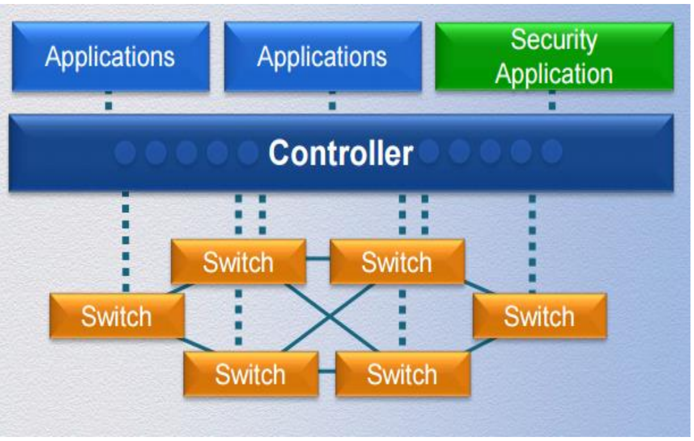

Fig 3. Security Policy [4]

The security policy is implemented to all the traffic by placing it in the application layer could be one possible solution to avoid security attacks. All Software Defined Networking flow should be checked against the overall security policy as shown in Figure 3 [4].

E. Isolation of Compromised Host

When a compromised host is identified, it can be isolated to avoid attacks.

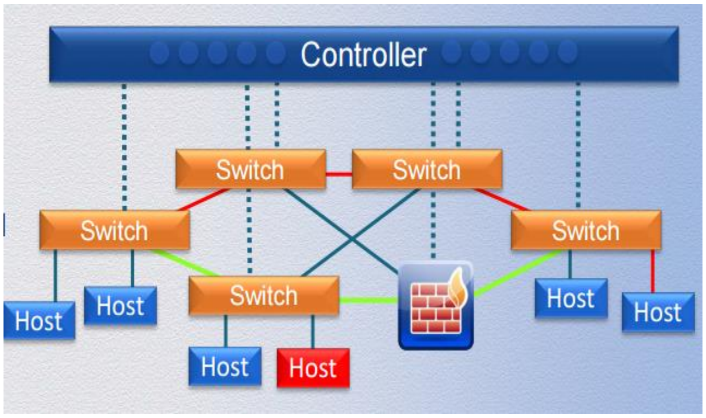

Fig 4. Isolation of Compromised Host [4]

F. Double Credential Verfication

Double credential verification refers to the need for two users to provide credential to access a control server. This is useful to avoid vulnerabilities on administrative stations, since hackers can reprogramming from single program

G. Logging

To figure out the cause of an attack or security breach and to investigate about the event, log that is secure and immutable can be used and needs to be stored in secure and remote environments.

H. Self-healing mechanisms

When there are hostile conditions, replacing components with new ones using self-recovery mechanisms will intensify the defense against vulnerabilities.

I. Replication

In case of any faults at either hardware or software levels, replication of controllers and applications as shown in figure 5 can avoid failure of the entire system. The malicious controllers or controllers can be quarantined. This improves the dependability by replication as shown in Figure 5 below.

J. Assigning switch dynamically with controllers

When we associate a switch with one controller, fault tolerance is not possible, since the switch fails along with the controller. Hence, a switch should be able to associate with numerous controllers to ensure fault tolerance and minimizing control delay by activating the controller that responds quickly.

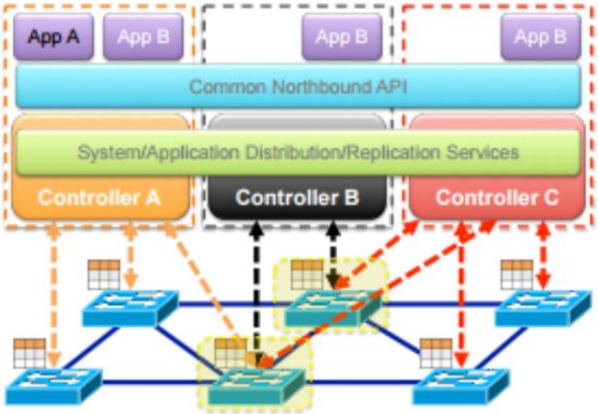

Fig 5. Replication of controller [5]

III. ISSUES AND PROBLEMS

The following are few security problems concerned with Software Defined Network.

A. *Attacks on Forwarding Plane*

1) Switch DoS

Since the switches have limited capacity, it cannot accommodate all the rules [6]. So a caching mechanism is implemented, where if a switch does not find a rule for the incoming packet, it stores the packet in the buffer. This type of mechanism makes switches prone to DoS attacks.

2) Packet Encryption

SDN follows flow-based forwarding scheme that allows packets with different payloads to be treated differently. . But, this scheme doesn't know how to manage with the encrypted packets, since packets can be encapsulated within other packets.

B. *Attacks On Control Plane*

1) Distributed DoS Attack

The control plane suffers from Distributed Denial of Service DDoS attack. In this attack, several hosts might flood the network switches with packets.

2) Compromised Controller Attacks

This attack happens when the attacker gains complete control over the controller and make sure that all incoming traffic are dropped and target on the victim to drain all of its resources.

IV. FUTURE TRENDS

SE – Floodlight is a more secure controller that ensures integrity between the security applications. SE-Floodlight can assign higher priority levels to the security applications.

Since controllers and protocols are being deployed newly, it is difficult to judge the future threats that will be aimed at the SDN architecture.

A. *Distributed Controller Design*

The research area involves scalability of the controller design. Even though the controller is centralized logically, it needs to be physically distributed [6]. This helps in attaining robust control plane.

B. *Information Centric Networking*

Information Centric Networking (ICN) is another future exploration area that improves both content delivery and content availability of the Software Defined Networking.

C. *Controller Interfaces*

The southbound APIs have been defined by ONF for communication between the controllers and switches. But the northbound APIs does not fulfill the basic standards. Though numerous controllers that act as a network operating system have been designed, proper application interfaces and their interactions have not been proposed to a well extent.

REFERENCES

[1] S. Hogg, "*SDN Security Attack Vectors and SDN Hardening*", Network World, 2016.

[2] D. Kreutz, F. M. V. Ramos and P. Verissimo, *Towards Secure and Dependable Software-Defined Networks*, 1st ed. Hong Kong, China, 2013.

[3] "*Identifying and addressing the vulnerabilities and security issues of SDN*", 2015.

[4] R. Hinden, "*SDN AND SECURTY: Why Take Over the Hosts When You Can Take Over the Network*", 2014. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] M. Dabbagh, B. Hamdaoui, M. Guizani and A. Rayes, *Software-Defined Networking Security: Pros and Cons*, 1st ed.

[6] Cs.wustl.edu, "*SDN: Development, Adoption and Research Trends*", 2016