SDN Security

Christin Wilson
cwils28@clemson.edu

***Abstract*—Software Defined Networking has expanded and has been established for creating and administering networks. It greatly improves the performance of a network compared to traditional networks. The main difference in a SDN network is that it is divided into two separate planes: data plane and control plane. As the SDN devices have found widespread use, the security concepts in an SDN network must be taken note of. This is a comprehensive survey of the security enhancements and the security threats that the SDN networks have brought about.**

I. Introduction

Software-Defined Networking is a networking technology that is used to improve the performance of a network by facilitating network management and an efficient network configuration. The traditional network architecture is decentralized with each device having to make its own decisions on sending a packet data. With SDN, the network becomes centralised, i.e., it divides the entire architecture into separate parts: the control plane and the data plane as shown in fig 1. The data plane is where the process of forwarding network packets happen whereas the control plane is where the actual network intelligence happens. The controller dictates the behaviour of the network. The complicated routing devices that are used in traditional networks turn to simple switches in SDN whose only job is to forward the packet data by following the policy instructed by the intelligent control system.

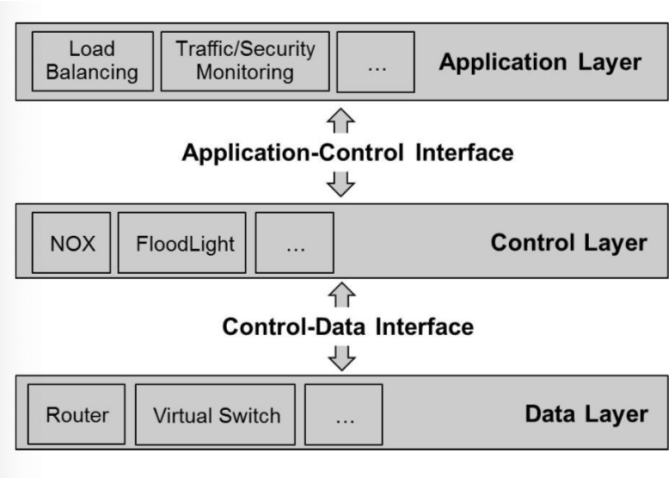

Fig. 1. SDN architecture illustrating the different layers

The existence of a separate control layer has benefits such as a central control point, error minimization, consistency, cost reduction and sophisticated traffic management. It is simpler and less error prone to configure the policies of the network than to work on each network device independently. It can also notice changes in the state of the network and take necessary changes and ensure that the high level policies are kept in place. It also simplifies the network functions since the controller has the global knowledge of the network state. SDN brings several promising additions such as simplicity availability, elasticity and programability to the network management. Today many of the major networking vendors like Cisco use and promote SDN networks. SDN uses the OpenFlow protocol for the control plane to determine the path of the packets through the forwarding switches. Eventhough several improvements are being brought to the SDN, one key aspect that requires attention is SDN security.
In this paper, we survey the various security risks and concerns that affect SDN. SDN does introduce new sophisticated network policies like security and dependability eventhough these have been a neglected topic.

II. SDN Security Pros

In this section, the characteristics that differentiate SDN from the traditional networks in terms of security are discussed.

A. Global Network View

The controller in the control plane has a global network view. This is one of the main security advantage of SDNs over traditional networks. Due to the centralization, all elements collect forensic traffic data and is collected by the controller. This is a much more complex procedure in traditional networks. These network forensics facilitate the quick and adaptive threat identification. Intelligence is harvested from the network, analysed, the policies are updated based on it and then reprogrammed for optimal experience. This brings a lot of security advantage:
1)Network-Wide Intrusion Detection: The SDN controller runs a network wide Intrusion detection system in order to check for malicious traffic happening between the network switches. This is possible due to the global network view and this is analysed from the satistics that are collected. In traditional networks this process is much more complicated and IDS provides much less effecient detection rates due to the limited visibility of the network. IDS operates in two ways:
(i) Misuse Detection: In this method, the existing and know attacks are analysed and a signature of these attacks are

created. The network behhavious is constantly monitored and if a match is found to any of the existing signatures, it reports the intrusion.

(ii)Anamoly Detection: In this method, the general basic behavioural data when the network is running smoothely without any malicious activity is recorded. This is when trusted applications are being run by trusted hostswithin the network. Here an intrusion is reported when any abnormal behaviour different from the profile stored is found.

2) Detection of Malaicious Switch behaviour: The global network view also helps in identifying malicious behaviour of the network switches. In cases where a network switch is dropping some or all incoming packets, identifying this behaviour is difficult in traditional networks. But in SDN due to the frequent reports that the switches has to provide to the controller. The reports will include the details of all the incoming, forwarded and dropped packets. The switches exhibiting malicious behaviour can be easily identified by analysing these reports. Even if the switch send wrong information in the reports by claiming to forward the incoming packets to other switches, the reports of the other switches can be checked to ensure this.

3)Network Forensics: The control plane logs the global network view over time. in case an attack goes unidentified, one can easily check this log in order to learn how the attack took place and defence mechanisms to defend against further attacks of that type can be created. It also helps in identifying the compromised hosts.

B. Self Healing Mechanisms: an example for this is conditional rules that was introduced in SDN. Certain rules are instaalled on the network switches such that it gets activated when a certain condition, that is usually related to a switch's collected statistics, is met. The activated rule will then guide the switch to respond according to the situation. This is especially useful to prevent denial of service attacks and for detecting botnets and prevent their attack. It has to be noted that OpenFlow does not enforce the switches to support conditional rules.

C. Increased Control Capabilities: SDN networks have more control capabilities on how the packets are being forwarded compared to the traditional networks. Due to the flow based scheme in SDN, Multiple header files are defined which contains information regarding how the packets should be handled in the network. The packets are forwarded not just by relying merely on the destination address. THe SDN controller Will have better control and decide what should happen to different type of packets based on its payload type, source address, or any other header field value. This will help in limiting malicious activity through the network by stopping them from entering or originating from any switch in the network.

III. Issues, Problems and countermeasures

We have already discussed the pros of SDN in terms of security. Now we discuss the security threats that a SDN network is exposed to. The separation of the architecture into the control plane and the data plane has created many attack surfaces that can be targeted for attacks. There are various points of attacks in a SDN network, i.e., attacks between data plane devices, on link connecting data plane devices, between control plane devices, on link connecting controller with data devices and on links between controllers. Some of these attacks are also applicable on traditional networks but some of these threats were introduced by the SDN networks. Also there are many security concerns related to the centralisation concept. If the controller is compromised, the whole network becomes defenceless and thus is the single point of failure. The various threats are :

A. Switch Denial of Service:

Switches have a limited capacity to store the rules that are produced by the controller and are to be followed in the network.Due to this, it is not possible for a switch to store all possible flaws in its storage. A caching mechanism is employed to counter this. When a flow which does not have a rule specified on the switch is encountered the switch stores the packet temporarily on a switch buffer and queries the controller for a suitable rule. Upon recieving the rule, the packet is processed based on it and the rule gets cached to ensure that future packets are processed without interruption. This mechanism makes switches vulnerable to the DoS attack. A attack can be carried out by flooding the switch with new flaws that the switch doe not have rules for thus making the buffer full by having packets wait until the required rules are obtained. This can lead to the dropping or delaying of certain packets due to overload and no storage space in the switch. Thus legitimate packets will not be processed thus causing the denial of service attack.

A solution against this attack is to store as many rules as the space allows in the switch rather than wait for the controller to send out rules each time. Also faster time of communication between the controller and the switch can make this wait unnoticable.

B. Control Plane DoS:

The denial of service attack can also occur at the controller layer. Similar to the previous case the attacker can flood the network switches with packets that have new flows. When all the network packets query the controller for rules, the controller can get overloaded and this can result in some of the legitimate requests to be dropped or delayed.

A solution to this attack is replication. Multiple physical controllers can be made use of in a single SDn network. These have to be connected with each other to ensure that all of them consist of the same rules and policies. Also the forward plane has to continue to work as if it is connected to a single controller. This technique will ensure that when a certain controller gets a lot of requests, some of these can be redirected to the other controller. The controller should be placed logically in the network so as to reduce the distance between the controllers and the switches.

C. Compromised Controller attacks:

These are the most severe threats to SDNs. As discussed earlier a successful attack on the controller can result in the entire

network getting compromised. If an attacker gets access to the controller, he will get complete access over all the switches. The attacker can bring changes to the rules and the policies. He can also make the switches to drop the incoming traffic or forward packets to wrong addresses. It can also be used to launch severe attacks on other targets.

Control replication can be used as a solution for this attack too. This is not completely efficient since if both the controllers will have the same vulnerabilities, the attacker will easily gain access to all the controllers once it gains access to one. In order to counter this, diversity has to be brought about in the different controllers to ensure that all the controllers are not compromised at the same time. Also some voting technique should be introduced such that when a conflict occurs in the rules received by the switches from different controllers, the rule which is sent by more number of controllers should be used. Also the encryption keys should be kept secured to ensure that these are not accessed by the attacker

D. Attack on the link between controller and switches:

Sending unencrypted messages between the controller and the switch can make the network vulnerable to man in the middle attack. The attacker can thus eavesdrop the information and the policies and rules being sent on this link. The attacker can also tamper the data sent and gain full access of a switch. Thus this link layer must be made secure from these attacks. A solution to this attack is to make use of some encryption techniques to encrypt the messages before sending it to the switches. Also timestamps should be made use of to ensure that the attacker does not hold back encrypted rules and then sent it later after the rules have changed. This is used to prevent replay attacks.

E. Attacks on vulnerabilities in switches:

A single switch can be made use of to create havok in the network by dropping or slowing down the forwarding of packets in the network thus deviating network traffic. Also packets can be forged and injected into the network to overload the controlled. Also requests can be sent to a specific destination switch and deplete its resources and bring it down. A solution for this attack is to use mechanisms to monitor, detect and manage the abnormal behaviours that the network switches show in a network.Also mechanisms like software attestation can help in defeating these attacks.

F. Attacks on and vulnerabilities in the administrative stations:

These attacks can occur in traditional networks as well. These attacks are used to gain access to the controllers. The threat is more eminent in SDN networks since a single compromised machine can cause a large effect here than in traditional networks. It is very easy in SDN networks to reprogram the entire network by gaining access to a single machine.

A solution for this attack is to use protocols requiring double credential verification. Also to guarantee a reliable state after booting, a assured recovery mechanism can be made use of.

G. lack of trusted resources for forensics and remediation

Trusted forensic reports can help to understand the cause of a detected problem and conduct recovery methods. For this, the data will only be useful if it can be trusted. Also safe and reliable snapshots are also required.

Inorder to ensure that the data forensics collected is trustworthy, the logs and tracing methods used should be inedible, i.e., they should be unmutable and secure. Also they should be stored in seperate safe environments where they will be secure.

H. Fake Controller: When a robust and secure controller platform is absent, an attacker can pose as a controller and can carry out malicious activities. To prevent this attacks, a security technology such as TLS with mutual authentication between the switches and the controllers can be used.

IV. Conclusion

In this paper, we have discussed the various pros and cons of SDN in the security perspective. Eventhough SDN networks are more secure compared to the traditional networks, there still are some security concerns that need attention. We have discussed various threats and their counter measures. Research on this subject is split into two general SDN research and OpenFlow. Eventhough OpenFlow is the most popular method of implementing SDNs, it was not originally designed for security. Also some of the benefits introduced by the SDN networks have itself brought several security vulnerabilities which require further study.

References

[1] Dabbagh, M., Hamdaoui, B., Guizani, M. and Rayes, A., 2015. Software-defined networking security: pros and cons. IEEE Communications Magazine, 53(6), pp.73-79.

[2] Kreutz, D., Ramos, F. and Verissimo, P., 2013, August. Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 55-60). ACM.

[3] Scott-Hayward, S., O'Callaghan, G. and Sezer, S., 2013, November. SDN security: A survey. In Future Networks and Services (SDN4FNS), 2013 IEEE SDN For (pp. 1-7). IEEE.

[4] Saxena, M., & Kumar, R. (2016, March). A recent trends in software defined networking (SDN) security. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 851-855). IEEE.

[5] Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M. and Rao, N., 2013. Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), pp.36-43.

[6] S.Shin,V.Yegneswaran,P.Porras,andG.Gu,AVANT-GUARD:scalable and vigilant switch flow management in software-defined networks, in Proceedings of the ACM SIGSAC conference on Computer & communications security, 2013, pp. 413424.