International Journal of Computer Science and Engineering Communications,
Vol.5, Issue.1 (2017):Page.1488-1494
IJCSEC.COM

Security Using Software Defined Network Paradigm

K.Jayanthi[1], N.Venkatesan[2.]
[1]Research Scholar, St.Peter's University, Chennai.
Jayanthi.sharathkumar@gmail.com
[2]Asst.Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai

Abstract-*Software-defined networking (SDN) is a great approach on computer networking which allows network administrators to manage the network service through the abstraction of a higher level of functionalities. This is to be done by de-coupling the systems which is making the decision about where the traffic is to be sent (to the control plane) from which the underlying systems that forwards traffic to the selected destinations (the data plane).SDN that requires some methods for the control plane to be communicated with the data planes. The important mechanism is the, open flow, is often misunderstood to be equivalent to the SDN system, but the other mechanisms could also be fit into the concepts. SDN architecture can be enabled, facilitated or enhanced by network-related security applications due to the controller centralized view of the networks, and the capacity to re-program the data plane at any state and any time. While the security in which the SDN architectures itself will remains an very opened questions that has been already studied a couple of times or in a couple of state in the research community, the following paragraphs will only be focusing on the security applications made possible or re-visited using SDN.*

Keywords: *data plane, distributed denial of service.*

I INTRODUCTION

SOFTWARE DEFINED NETWORKS:

Several more researches worked on SDN which is already be investigated through the security applications built in upon the SDN controllers, with different aims in the mind. Distributed Denial of Service (DDoS) detections and mitigations, as well as the botnet and the worm propagations, are some of the concrete use-cases of in such a applications: basically, the idea consists of the concept of periodically collecting the network statistics from the forwarding plane of the networks in which the standardized manner (e.g. using Openflow), and then to apply the classification algorithms on those statistics in the order to detect any networks anomalies. If an anomaly is to be detected, the application instructs the controllers on how to re-program the data plane in order to mitigate it. Developing the applications for software defined networks requires the most comprehensive checks of the possible programming errors. Since the SDN controller applications are the mostly deployed and used in large

scale scenarios of a programming model by checking solutions requires scalability. These functionalities are provided among others through NICE. SDN is an approach to computer networking that allows administrator to manage network services through abstraction of higher level functionality. The movement to software-defined networks brings the dramatic and interesting changes in the network design and the security. As the long terms ago, the corporations will be benefited from more intelligent and the secure networks management. In the short period of time, new networking features can have more open security holes in which the hinder the rollout of the software defined networks. Software-defined networking (SDN) is an architecture created for the purpose of the network communication of data should to be dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's and upcoming applications. SDN architectures de-couples the network controls and forwarding functionalities, enabling network controls to becomes the directly programmable and the underlying infrastructures to be abstracted from the applications and network services.

II ARCHITECTURE OF SOFTWARE DEFINED NETWORK:

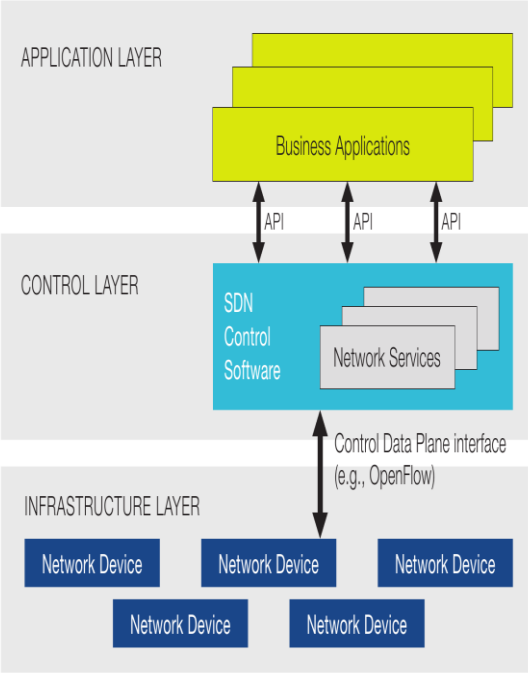

Figure 1. Architecture of software defined network.

SOFTWARE DEFINED NETWORK TOPOLOGY:

The SDN topology is the one which separates the control plane from the data plane. The controller now can manages the traffic flows through the various paths in the network without the limitations from the physical device and the proprietary software implementations. Network flows are to be typically (but not always) controlled with the open flow protocols. Traffic patterns are also be changed, from North/South (user to data center) to East/West (within the data center). Traditionally, 75% to 85% of corporate traffic are to be flowed over the enterprise network and about 10% to 50%

moved in the data center. Today, those numbers which are to be reversed, due to the virtualization and converged architectures.

Threats, inside and out:

Software defined network security deals with external and internal threats.

External threats:

External threads are the individuals trying to get into the network who do not belong there -- are becoming more sophisticated. Traditionally, tools such as firewalls, error controller, issue fixing tools intrusion-detection systems and intrusion-prevention systems, sandboxes, and deep packet inspection data safe.

Internal threats:

Internal threads are the threads which are increasing in numbers and complexity. Businesses which needs to be monitor the information, as it would moves the system inside, e.g., between two virtual machines (VMs) or from a server to a storage system or from client to server system. Large volumes of traffic can move at a very incredible speeds as fast as the data flows among virtual systems, and the traditional tools often cannot keep pace.

NETWORK SECURITY CHALLENGES:

IT infrastructure is rapidly moving to the cloud, creating a dramatic technology shift in the data center. Security concerns are consistently identified as a major barrier to this data center transformation. Data center resources including hypervisors, storage devices, servers, switches, and routers must be secured. Existing security strategies can be successful at minimizing many of the security risks in the data center

III CURRENT SECURITY SYSTEM:

Currently, the available security solutions of the software defined solutions are, however, difficult to deploy, manage, maintainability, reusability, program, scale, and secure. Security solutions of SDN, often struggles to provide such a quick and automated threats mitigation across equipment from multiple vendors. Consistently the security policies are very difficult to be administered across computation, storages, and the network domains and the multiple data centers. No solutions today will allow for completeness of the data security.

The Implications of SDN on Network Security:

Open Flow-based SDN offers a numerous of attributes that are to be particularly well suited for the implementation of a highly securable and manageable environment:

The flow paradigm is an ideal for the security processing because in which it offers an end-to-end, service-oriented connectivity model of such network that is not bound by traditional and untraditional routing constraints. Basically centralized controls which allows for effective and efficient performance and threats monitoring across the entire network. Granular policy management which can be based on applications, services, organizations, and geographical criteria rather than physical configurations. Resource-based security policies enable consolidated managements of diverse devices with various threats risks, from highly secure firewalls and security appliances to access devices.

Dynamic and flexible adjustments of security policy is provided under programmatic control. Flexible path management achieves rapid containment and isolation of intrusions without impacting other network users. By blending historical and real-time networks state and the performance data, SDN facilitates intelligent decision-making, achieving flexibility, operational simplicity, and the improved security across a common infrastructure.

IV SDN SECURITY:

Secure SDN Architecture

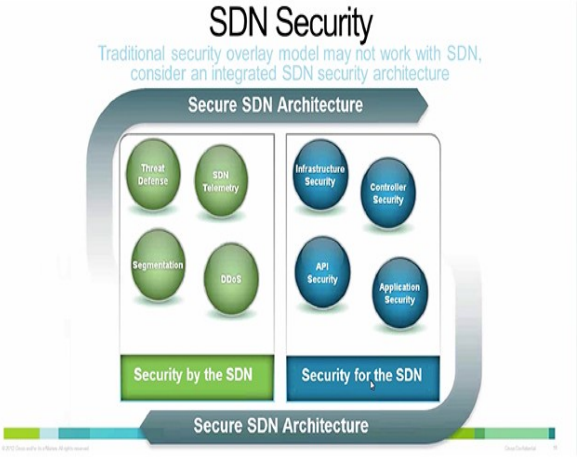

Figure 2. Architecture of secure software defined network

SDN security benefits:

"If someone is not able to handle or pay such attention to [the controller], it becomes an extra-ordinarily a great and high profit goals for each of an attacker, who could be pay more interest and very easy compromise [it], modification of some of your codes based on the related networks and re-scripted controls of your traffic in such a perfect or exact way that it's ex-filtrating data or stashing data somewhere where an attacker can sniff it," said Dave Shackle ford, security consultant with Voodoo Security and leads faculty member at IANS."There are so and large many opportunities for an attacker or the hackers to make changes or to hack data to the whole underpinning of your networks traffics behavior just by modifying your controller. We've never really had that before. Even traditional network management tools didn't give you the flexibility to dynamically change the behavior of a network on a node-by-node basis." The programmability of SDN controllers which presents a double-edged sword. Engineers can install security applications on the controller's northbound interface to open up the new ways to be applied for the security policies on a networks. Those applications will instruct the controllers to be used as the switches and routers that it controls as policy enforcement points. By having the free-moving network of SDN, engineers are able to change the rules by having a quick, high-level view into all areas of the network and being able to modify the network. This freedom and control also allows for better security of your systems .Able to be quickly change the things in the networks enables managers to perform traffic shaping and the QoS of packets in a more securable matter.

SDN security concerns:

Some of the Security based issues to beware of when implementing SDN:

The first priority of software-defined Networking (SDN) security concerned with the solutions on going to emerges only around the controller itself. The controllers can only be considered the main one that means the brains of the switching or routing, which allows the control panel from which each of the system is to be centrally managed.

Steps in Security using SDN

Secured through the following steps:

Knowing and auditing who has to access the controllers and where it to be the exact resides on the network is a big security system concern. Verifying the security between the controller and end nodes (routers or switches) .Verifying that there is highly available in the controllers. To Verify, that there is everything that comes out of the system is logged in or logged off. When implementing SDN, verifying that the organization's SIEM, IPS and any other filters technology that might blocks or logs changes is updated accordingly.

Strategies needed for software-defined networking security:

Networks managers and the admin must learn to set security level appropriately in the new and the dynamic environments .Ideally, there will be many pre-provisioned security policies logic inside a policy management systems.

This approaches would be defined the rules of what is to be denied or to be allowed with certain subscribers, applications, devices, locations, network access methods and the network characteristics on each of the network segments

SDN SECURITY:

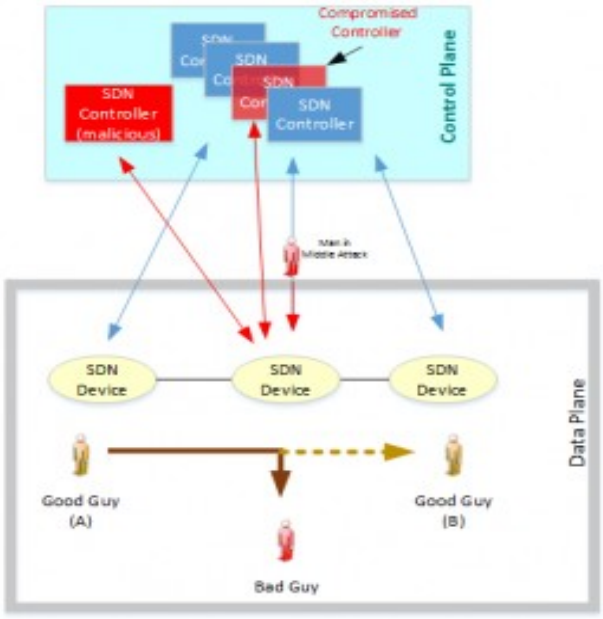

Figure 3. SDN Security

Security in traditional architecture networks:

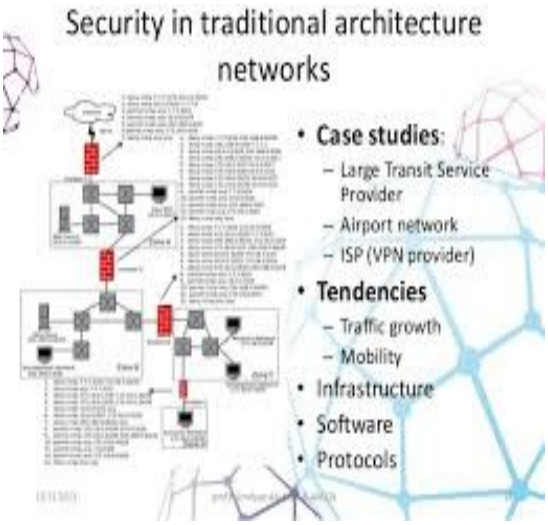

Figure 4. SDN Security in traditional architecture networks

V RESULT:

The limitation of this paper to wired networks. SDN is independent of the physical media, as so abstraction of the network elements makes this implicit. However, we will not be explicitly explore the implications for mobile/wireless networks here in this paper. Interested readers can able find relevant an earliest SDN-enabled for mobile networks.

So, While not specifically SDN, as a matter of scope it is important to make the clear relationship with network function virtualization (NFV).The dynamic data transfer from one network to another can be safer and the hackers could not break the data because the tool perform the exact code match in the particular sending the data.

VI CONCLUSION:

Software-defined networking is a raising technology that may allows for granular security by giving an administrator a complete view of the enterprise network. However, by giving the controller of the centralized management over networks nodes to push down the exact changes to these systems, it becomes imperative that the security around this system is locked down. This system is only the brains of SDN, and without the proper security wrapped around it, the network becomes the complete vulnerable to malicious attacks and (or) or accidental changes, both of which can take a network down. So, now this is the time for organizations to ensure that security is a primary consideration in the design, deployment and management of SDN.

REFERRENCES:

[1] Open vSwitch. http://openvswitch.org/.
[2] Openflow - enabling innovation in your network. http://archive.openflow.org/. Open Networking Foundation.
[3] The SwitchWare Project. http://www.cis.upenn.edu/ switchware/l. University of Pennsylvania.
[4] The xen project. http://www.xenproject.org/.
[5]D.J.Bernstein.SYN Cookies. http://cr.yp.to/ syncookies.html
[6] P. Bosshart, D. Daly, and M. Izzard. Programming Protocol-Independent Packet Processors. arXiv preprint arXiv:, pages 0–6, 2013.
[7] M. Casado, M. Freedman, and J. Pettit. Ethane: Taking control of the enterprise. ACM SIGCOMM, 2007.
[8] A. Curtis and J. Mogul. DevoFlow: scaling flow
management for high-performance networks. ACM SIGCOMM, 2011.

[9] A. Dixit, F. Hao, S. Mukherjee, T. Lakshman, and R. Kompella. Towards an elastic distributed SDN controller. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN ’13, page 7, 2013.

[10] N. Feamster, J. Rexford, and E. Zegura. The Road to SDN. ACM Queue,