IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue-16, May 2019 E-ISSN: 2347-2693

Effectiveness of Security in Software Defined Networks

B. Parvathi Devi[1*], V. Vallinayagi[2]

[1]Dept. of Computer Applications, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu
[2] Dept. of Science, Assistant Professor, Sri Sarada College for Women, Tirunelveli, Tamil Nadu

Corresponding Author: parvathikeerthi82@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si16.122125 | Available online at: www.ijcseonline.org

Abstract— Software Defined Networks are the new standard in networking. ONF [Open Networking Foundation] contributes a high level architecture for SDN. It has three layers, they are Infrastructure layer, control layer and application layer.[1] From the ONF we gets a well-defined definition for SDN which is as follows, "In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications" [2]. The network security in the SDN architecture is improved by the centralized control over the network and controls the traffic in run time. This paper analyse and produce the importance and effectives of the SDN architecture for future networking.

Keywords— SDN , ONF, Network security**.**

I. INTRODUCTION

SDN is a new technique in networking architecture. Designing the SDN architecture is not the easiest task. In this architecture a software program controls the overall network and it is responsible for decision making like transferring packets from source to destination system.[3]. This controlling software is called Controller. This SDN contains three layers Infrastructure layer, Control layer and Application layer.

Infrastructure Layer: This layer consists of physical switches and routers. These physical devices are accessible through an open interface to switch and forward packets. These physical devices forms underlying network to forward network traffic. This layer is also referred as Data plane.

Control Layer: In the SDN architecture, this layer is in the middle position. It contains Software built controllers which providing a control functionality through open Interface. The Southbound, Northbound east/west bound are the three interfaces allow the controllers to interact among them. [4]

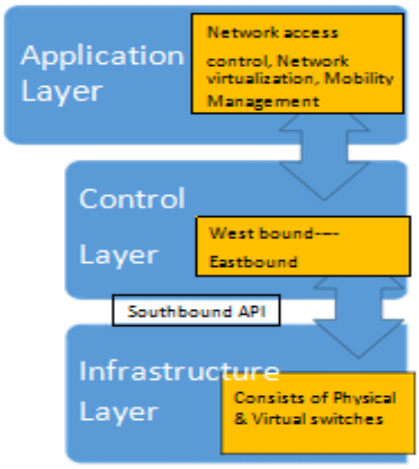

Fig 1.1 Layers in the SDN

Application Layer: In this layer the user can create their own applications which can be related to automation in networking, managing the network etc. These end-user commercial applications get the SDN communications through the network services.[4]

This paper gives a detailed review of importance, effectiveness and need of SDN architecture. The main effective of this architecture is Intruder Detection. Atlast this paper gives an idea of how the intruders are detected and deleted from the network.

II. EXISTING ROGRAMMABLE NETWORKS

In the mid of 1990's the Internet starts to its success. After the fast growth of the Internet networking structure also modified to connect more number of systems. In that time two control software were designed and they provide open interfaces. They are Open signalling [OPENSIG] and Active networking.[5]

Open Signalling [OPENSIG]: The important aim of this working group is to separate the control and data plane of networks, and put on the concept of programmability in ATM networks. This concept leads to further in research areas. Based on this OpenSig method, multiple control architectures are managed by the multiple switch controllers over the same physical ATM network.[6]

Active Networking: This type of networking was mainly supported by DARPA. This Active networking's main goal is also programmable networks. This type of architecture defines three layer stack on active nodes. They are Bottom , middle and Top layers[7] The SDN concept come out from the active networking concept only.

III. INTRUSIONS IN THE NETWORK ARCHITECTURE

A.Attacks in the Virtual Machines
Hypervisor or Virtual Machine Monitors are easily hacked by the attackers by the compromising hypervisor. Intruder first targets the virtual machine services like create/delete clone and migrate to use them by misusing the zero-day vulnerabilities in virtual machines [8] Several websites may damaged based on this virtual server [9].

B. User to root attacks
In this type the hackers, hack the system with the user account and try to get the information inside a system by misusing vulnerabilities. This attack interrupts the reliability of cloud based systems [10].

C. Insider Attacks
Here the hackers are the official users in the path but they misuse their rights and try to change some details. [10]

D.DoS (Denial of Service) Attacks
It is a type of attack which makes the resources unavailable to the valid users.[11] This type of attacks are challengeable for SDN architecture.

E. Backdoor path Attackers
Here the hackers try to attack the infected machines continuously and hack the data . This is called Backdoor attack

IV. SECURITY IN SDN PLANES

In this section we discussed about the security in application, control and data planes

1.Application Plane Security
SDN architecture allows the application to interact and manage the network devices through the control layer. The whole view of the network resource information is provided by the control plane to SDN application plane, and the applications must work in their limits and have the control to network resources

PermOF is a permission control system used in the application plane to control the permission access like read, write and notifications[12]

2.Control Plane security
In the SDN architecture the controller is responsible for the whole network. This controller implements the functionalities of the control plane[13]

Advanced Messaging Queuing Protocol (AMPQ)[14] is used by the Floodlight openFlow controller which is implemented in the top of the Distributed SDN control plane (DISCO).It monitors the inter domain and intra domain functionalities of the network. The controller placement is the biggest task in the control plane, for that we uses the most optimal algorithm for controller placement. For example simulated Annealing algorithm, generic Probabilistic algorithm15]

3.Data Plane Security
The data plane must protected from malicious applications which can change or alter the flow rules in the data path. Hence, fine-grained security implementation appliances such as authentication and authorization are used for applications. FortNox [16] is one such platform that enables the NOX OpenFlow controller to check flow rule inconsistencies in real time and authorize OpenFlow applications before they can change the flow rules.

VeriFlow [17] is the network debugging tool used to find defective rules interleaved by SDN applications and protect them from causing irregular network behaviour.

These are the techniques used in the SDN planes to maintain the security in the network architecture.

V. CHALLENGES IN SDN SECURITY

In the growing technology world the needs of every technique must be updated by the provider, So there is some challenges in using the SDN network architecture. Here we consider only the two challenges and their remedies They are as follows,

1.Security and Scalability
Scalability is the biggest task faced by the SDN. In SDN the size of the network is increased then the volume of control traffic destinated to the central network increases. So flow of time is also increased [18] Lack of scalability leads to control plane starvation. [19]

Most of the SDN threads, aim to conciliation the handiness of the control plane. Thus more controllers are the solution to the security in the control plane. But multiple controllers result in cascading failure among them. So correlate the scalability and security in the SDN architecture is reduce this type of problems. *2. Control the Data plane Intellect Tradeoff* In SDN one controller or pool of controllers provides the control plane services to others is result in latency problem in exchange the network information. Therefore intelligence tradeoff is the solution to reduce the switch dependency on the controllers. [20]

VI. CONCLUSION

In this paper we discussed the SDN architecture in detail, and discuss some of the past programmable networks and its functions in the network architecture. Compared to them SDN gives the security of network through over-all visibility of the network state. In SDN, to apply security polices, a common distribution layer collects information about security desires of different services, resources and hosts, and disseminates security establishing commands. SDN is the new architecture comes with strong and scalable security application, and also it have some new type of security tasks. However, SDN aims at bringing modernization in communication networks and thus, programmed security appliances will be established to allow fast anomaly detection and rapid reaction for protection.

REFERENCES

[1] M. D. Yosr Jarraya, Taous Madi, "A survey and a layered taxonomy of software-defined networking," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 4, pp. 1955–1980, Fourth Quarter 2014.
[2] S. Sezer, S. Scott-Hayward, P.-K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, July 2013.
[3] S. Namal, I. Ahmad, S. Saud, M. Jokinen, and A. Gurtov, "Implementation of OpenFlow based cognitive radio network architecture: SDNR," Wireless Networks, pp. 1–15, 2015.

[4] M. D. Yosr Jarraya, Taous Madi, "A survey and a layered taxonomy of software-defined networking," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 4, pp. 1955–1980, Fourth Quarter 2014.
[5] A. T. Campbell, I. Katzela, K. Miki, and J. Vicente. "Open signaling for ATM, internet and mobile networks (OPENSIG'98)." ACM SIGCOMM Computer Communication Review 29.1 (1999): 97–108.
[6] J. E. Van der Merwe, S. Rooney, I. Leslie, and S. Crosby. "The tempest-a practical framework for network programmability." IEEE Network 12.3 (1998): 20–28.
[7] N. Shalaby, Y. Gottlieb, M. Wawrzoniak, and L. Peterson. "Snow on silk: A nodeOS in the Linux kernel." *Active Networks*. Springer, Berlin (2002): 1–19.
[8] NIST: National Vulnerability database, http://web.nvd. nist.gov/view/vuln/ detail ? vulnId=CVE-S2009-3733; 2011.
[9] D. Goodin, "Webhost Hack Wipes Out Data for 100,000 Sites ",http:// www.theregister.co.uk/ 2009 /06/ 08/ webhost_attack, 2009
[10] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan,"A Survey of Intrusion Detection Techniques in Cloud", Journal of Network and Computer Applications 36 (2013), pp. 42-57.
[11] S. Shin and G. Gu, "Attacking software-defined networks: a first feasibility study," in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 165–166.
[12] X. Wen, Y. Chen, C. Hu, C. Shi, and Y. Wang, "Towards a secure controller platform for OpenFlow applications," in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 171–172.
[13] T. Tsou, H. Yin, H. Xie, and D. Lopez, "Use-Cases for ALTO with Software Defined Networks," 2012.
[14] Advanced message queuing protocol. [Online]. Available: http://www.amqp.org
[15] Y. Hu, W. Wang, X. Gong, X. Que, and S. Cheng, "On reliabilityoptimized controller placement for software-defined networks," Communications, China, vol. 11, no. 2, pp. 38–54, Feb 2014.
[16] security enforcement kernel for OpenFlow networks," in Proceedings of the First Workshop on Hot Topics in Software Defined Networks, ser. HotSDN '12. ACM, 2012, pp. 121–126.
[17] A. Khurshid, W. Zhou, M. Caesar, and P. B. Godfrey, "Veriflow: Verifying Network-wide Invariants in Real Time," SIGCOMM Comput.Commun. Rev., vol. 42, no. 4, pp. 467–472, Sep. 2012.
[18] A. Tootoonchian and Y. Ganjali, "HyperFlow: A distributed control plane for OpenFlow," in Proceedings of the 2010 internet network management conference on Research on enterprise networking. USENIX Association, 2010, pp. 3–3.
[19] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Avant-guard: Scalable and vigilant switch flow management in software-defined networks," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS '13. ACM, 2013, pp. 413–424.
[20] A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sherwood, "On controller performance in software-defined networks," in USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services (Hot-ICE), 2012.

Author's Profile

B.Parvathi Devi pursued Bachelor of Science from Sri Sarada College for women, Tirunelveli, affiliated to Manonmaniam Sundaranar University, Tamil Nadu in 2003 and Master of Science and Master of Philosophy in the same university in 2006 and 2007. Her main Research work focuses on Network Security in the Edge computing with SDN architecture. She is currently pursuing Ph.D and working as an Assistant Professor, Department of Computer Applications, Sri Sarada College for Women , Tirunelveli since 2009.

