Vulnerability of SDN Network Architecture and Proposed Countermeasures on Enhancing Security

Nitheesh Murugan Kaliyamurthy, Swapnesh Taterh, Suresh Shanmugasundaram

Abstract — ***The current problems raising as a horizon in the computational and networking sector is based on the unimaginable increase of high numbers of users which in turn results in high data traffic, limitations over products which are vendor specific, incurring high expenses in maintaining the existing network. This dilutes a major part of the beneficiaries in the sector to move towards Cloud Networks. All these happenings in the past has quietly increased the risks and challenges in the aspect of security considering both data and the infrastructure accommodating the data. In an attempt to address almost a major portion of the existing above said problems, Software Defined Networking was highly anticipated, however, it was considered as a theoretical approach. After the implementation of SDN networks by industrial giants like Google, the SDN concepts again managed to reach the safer hands of the researchers in the movement of enhancement. A very rapid and high speed research work has been initiated by researchers all around the globe in analysing the risk factors and implementation barricades stated in the Software Defined Networking architecture. The research work focus on adding values to the Quality of Service, Latency, Load Balancing and most importantly the security aspects in various metrics of the Software Defined Networking Architecture. The odd man out architecture of Software Defined Networking by decoupling data and control plane allows the network to be configured and maintained in a real time scenario pertaining to pose a complete view of the network and its flow. The fact that is considered as an advantage itself is a factor of question in the case of security in the overall SDN architecture. This paper focuses on a detailed view of SDN architecture with the existing security feature and continues with the expected threats and classifying the weak points in the SDN. This paper also briefs about the pros and cons of the existing applications in the SDN architecture.***

Keywords: Software Defined Networking, Mininet, SDN, Data Plane, Control Plane, OpenFlow, Attacks, DDoS, TAN, Traditional Architecture Network

Manuscript published on November 30, 2019.
* Correspondence Author

Nitheesh Murugan Kaliyamurthy*, PhD Scholar, Amity Institute of Information Technology, Amity University, Jaipur, Rajasthan, India. (Email: k.nitheesh.murugan@gmail.com)

Dr. Swapnesh Taterh, Associate Professor, Amity Institute of Information Technology, Amity University, Jaipur, Rajasthan, India. (Email: staterh@jpr.amity.edu)

Dr. Suresh Shanmugasundaram, Professor, Faculty of Engineering and Applied Sciences, Botho University, Botswana (Email: suresh.shanmugasundaram@bothouniversity.ac.bw)

I. INTRODUCTION

Software Defined Networking is the most trending topic nowadays for any researcher trying to address the problems faced in the current networking platform. The growth of IP users in the network is extremely raising in an unthinkable numbers and as a matter of fact, its dependencies such as data flow, sensibility and sensitivity of information in the network also eventually increases. Even though consistent research works are happening to address the problems raised in the existing network architecture, it is taking the domain into a narrow scale of focus rather than a broader enhancement. The IP Network architecture, since implementation is lacking the pace in the growth by focusing on a narrow path in the last 15 years while other domains leverage significantly (Kirkpatrick, 2013). Consistent development in the metrics of speed, data handling, QoS, Load Balancing Algorithms and data security increased rapidly is a positive sign (Kaliyamurthy Nitheesh Murugan, 2019) in the existing network architecture. However, these growths were not up to the mark to meet the requirements of cloud computing, resource sharing in enabling a centralized facility. Depletion of IPv4 Addresses and migration towards IPv6 Addressing is one of the valid evidence to facilitate the existing network architecture's growth. Manual configurations in the networking devices still remain the same from the beginning unlike other domains which are comparatively having customization facilities as per the requirements of the user. This is also a point to consider, moving into a diversified path rather than moving in the same direction (Kirkpatrick, 2013). Software Defined Networking, mainly eyed due to its decoupled architecture in both industry and academic fields. SDN provides a flexible network flow based on the network requirement due to its common policy configurations instead of manual configurations, resulting in reduced operational cost (NetworkSecurity, n.d.). SDN also addresses implications raised because of closed networks and vendor specific proprietary implementations commands in the traditional networks (TAN) by enabling to create new and required network services. This is possible because of the intelligence and flexibility provided to the control plane by decoupling it from data plane (NetworkSecurity, n.d.). SDN is likely to address a majority of current issues in the existing network architecture in addition to its feasibility towards cloud based operations, remote access, virtualization etc.,

Retrieval Number: D5266118419/2019©BEIESP
DOI:10.35940/ijrte.D5266.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(Kirkpatrick, 2013) (Raphael Horvath, 2015). SDN considered being the next diversified future technology in the networking community because of its customized and centralized architecture, there are various aspects of SDN which requires furthermore concentration. The ultimate aim of any networking architecture being delivery of data from any source to any destination in a faster, efficient and safer method (Nitheesh Murugan K, 2016), the existing IP Architecture and the SDN facilitates various techniques such as latency techniques, QoS, Load balancing Algorithms and Build-in Security Policies. Many researches are happening in both Industry and Academic domains in addressing the above goal. Out of all techniques concentrating the faster delivery of data, safer delivery of data is one of the raising key concerns which require high attention. Security in a network still remains a raising concern as it is comparatively slow with the growth of networks (Seungwon Shin L. X., 2016). Concentrating on the security aspects of a SDN Network, a wider and rationale view approach is required. Generally, to improve security in any environment, the vulnerabilities in that environment are needed to be identified. Based on the vulnerabilities, the weak point in the environment needs to be identified. Based on the analysis of the identified vulnerabilities and weak points, the security enhancements are to be designed and implemented. This paper reports on the above stated wider and rationale view approach, by stating the importance of the security needs in Software Defined Networking Architecture in part II. Furthermore, analysis on possible threats and attacks based on SDN weak points is discussed in Part III. The existing security applications and its limitations are discussed in Part IV. This study concludes with the required steps to be taken in overcoming the limitations of Security Applications.

II. SECURITY IN SDN

Security is a key factor in any modes dealing with information. “Information is wealth” - a general quote suits aptly now a days anticipating the sensitivity of data being transferred through various networks. The volume of increasing users eventually increases the amount and importance of data. A variety of information such as Financial, Personal, Private, Current happenings pass through the network anonymously. This increases the number of attacks for the information over the networks these years. Even though various security methods and measures were imposed in the networks to secure the data, the attacks place themselves in a more sophisticated position in intruding the network and accessing the data (Jerome Francois, 2014). This current situation enhances the already said quote into “Securing information is wealth”. There are a lot of investigations happening over decades in handling the attacks (Jerome Francois, 2014). Security has seen a wider and broader growth by gaining attention in all the domains due to its importance of securing the information. Network security falls under the umbrella of Cyber Security which already has a perfect take off (Wenfeng Xia, 2015). Software Defined Networking, which impressed the networking domain with its decoupled architecture, facilitates programmable network configuration and simplifying the complexity in network configuration and network modifications as per the requirement in the network (Diego Kreutz, 2013). This advantage of SDN, poses itself a wide exposure to the attacks, as the controller which is considered as an intelligent device can easily be exploited, compromised and deployed with malicious applications (Kaliyamurthy Nitheesh Murugan, 2019). Comparing with the traditional network architecture (TAN) where the Control and Data Plane are interlaced, the attacks over the network can happen even with a single compromised router. By isolating the control plane might enhance and improve the reliability of the network (R.L., 2014) whereas, the SDN already has its controllers away from the routing devices focusing on an efficient control over the network by initiating control plane dynamic flow rule enforcement to the data plane whenever required (Seungwon Shin G. G., 2013). SDN is capable of implying its own software applications enhancing the security of its network without any expensive infrastructure (Kaliyamurthy Nitheesh Murugan, 2019) like firewalls and proxy servers in securing the physical devices (Wenfeng Xia, 2015). The main advantage of moving towards Software Defined Networking is because of its decoupled control and data plane architecture which provides a centralized view over the network. This helps to imply policies and configurations in the network negotiating the security breaches then and there which eventually voids the need of expensive devices and reduces the cost of vendor dependent infrastructure (Wenfeng Xia, 2015) (Kaliyamurthy Nitheesh Murugan, 2019). Possible security lapses in the network due to Distributed Denial of Service Attacks, Intrusion Prevention, Spoofing, Tampering, Repudiation, Information Disclosure and Elevation of Privilege (A discussion with Amin Vahdat, 2016) can create serious problems in the aspect of security which in turn fails the purpose of implementing the decoupled network architecture (Seungwon Shin G. G., 2013). Security in Software Defined Networking will be an added advantage in its deployment, considering the enormous amount of data flow and its design of forwarding data packets. The SDN Architecture, not only due to its cost saving feature, but also for its robust performance and customized functionalities, supersede the existing network architecture, needs special focus on improving the security based on the specific type of attacks and the weak points in the architecture (R.L., 2014).

III. ANALYSIS OF THREATS AND CLASSIFICATION OF WEAK POINTS IN SDN

Software Defined Networking, a new variant in the network domain emphasizing on centralized control over the networks and feasibility to network programming is posed to new threats other than the threats and attacks experienced in the existing network architecture. The possible threats and attacks in a Software Defined Network are classified based on its network design as the controller itself is vulnerable to different kinds of attacks (Kannan Govindarajan, 2013). However, SDN has the capability to react instantly to detect and counter-attack threats like low-rate burst, distributed denial of service attacks by analyzing the traffic flow in the network.

In those cases, the analysis of data traffic also may be directed to any intrusion prevention system available in the network for further investigations. The attacks can be prevented from entering the network by implementing packet forwarding rules to the forwarding devices (Wenfeng Xia, 2015). These forwarding rules are sent from the SDN controllers which if compromised will let the entire network to be vulnerable to any kinds of threats and attacks. Workload Changes and Misconfigurations are the other possible threats which are posed in SDN as these attacks use the passively collected open flow control messages to detect the active network flows (Kannan Govindarajan, 2013). In an SDN, the key to protect the network is to analyze the weak points in the architecture. In the aspect of security, the strength of SDN is considered as the weak points which are viable to possible threats and attacks. SDN relies on software applications in controlling the network by imposing flow rules based on the incoming and outgoing data traffic is one point which is posed to be attacked. Discovering and modifying the flow rule, imposing new flow rules pose viable threat to the network. Handling of credentials for logical networks in the data plane is another weak point which needs attention. Unauthorized Access of the Controller, Denial of Service, Misconfigurations, Lack of network visibility are considered as other major threats and which can poses viable attacks in the network (Wenfeng Xia, 2015). Another threat to the network is the Man in the Middle attacks which might be from the internal or external sources of the network (OKAMURA, September 2013).

Though, these attacks poses comparatively limited effect in the network with the other types of attacks discussed earlier in this section, they still remain as a threat to the network. These attacks capture the data packets from the distributed controllers and attempt to change or inject irrelevant information (OKAMURA, September 2013). The SDN networks designed in the perspective of centralized architecture might have multiple controllers which gains access to the data plane in the network along with their applications. The controller holds the entire control over the network, providing permission to the applications in imposing flow control rules based on the network state. Gaining access to the network resources and manipulating its operations will be viable for any attackers when a controller is exposed (Scott-Hayward, 2015). Securing the network is a highly challenging task which needs appropriate identification of weak points in the network, which may vary based on the structure of the network. Identification of the weak points and strengthening them in order to secure the network needs a network to impose confidentiality, integrity and availability of information (Scott-Hayward, 2015). The security factor in Software Defined Networking is a combat between the positives of the network. The attractive and progressive evolutions of networking architecture, the key advantage of SDN networks itself pose increasing threat (Diego Kreutz, 2013).

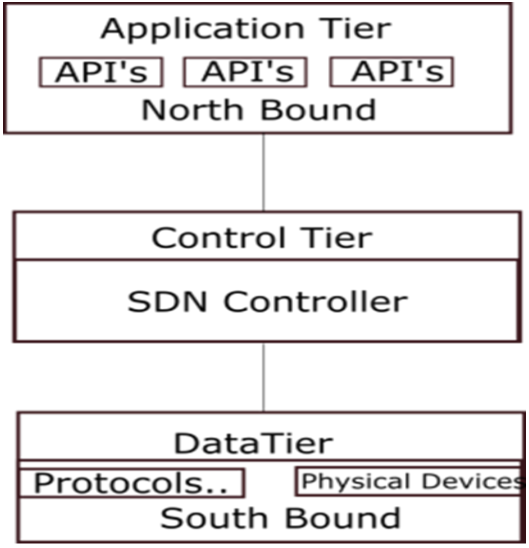

Figure I: Overview of SDN Architecture in Security Prespective.

Improving the Dynamic Flow control, network wide visibility, programmability (Seungwon Shin L. X., 2016)with additional check points without increasing the work load on the physical devices might address the problems related to security.

Type of Attack	Weak Point in the Network
LOW-RATE BURST & DISTRIBUTED DENIAL OF SERVICE	Control Tier
DATA MODIFICATIONS & LEAKAGES	Application, Control & Data Tier
UNAUTHORIZED ACCESS OF THE CONTROLLER AND API's	Application & Control Tier
LACK OF NETWORK VISIBILITY	Control & Data Tier
CONFIGURATION ISSUES	Control & Data Tier
MAN IN THE MIDDLE ATTACKS	Control Tier

Table I: Types of possible attacks and the Weak Points in the Network

The table 1 clearly summarizes the different types of attacks possible and its weak points in the Software Defined Network architecture. Matching the Figure 1 and table 1 will give an overview on the exact weak points and the possible attacks in the network.

IV. MITIGATING THE WEAK POINTS IN SDN & RESULTS

The possible weak points and the type of attacks were discussed in the previous part leveraging us to discuss the available security applications to secure the network. There are a lot of researches happing in the recent past to improvise the security aspect which is considered as the prime factor in deploying Software Defined Networks. This part analyses the existing security applications available and its limitations in a different perspective further lending hands to the researchers to concentrate on those areas where it needs to be concentrated. NetFuse (Ye Wang, 2013), Fresco (Seugwon Shin, 2013), Active Security, Avant-Guard (S. Shin, 2013), SDN-RTBH, CloudWatcher, DDoS detection, SANE, VAVE are few applications dealing to address the security issues with the Software Defined Networking Architecture (Kaliyamurthy Nitheesh Murugan, 2019). Let us funnel up these applications with the threats it is addressing along with their limitations, which will provide an eagle view's perspective in looking towards the problem.

The decoupled architecture in Software Defined Networking may lead to a Denial of Service Attacks either on the controller or on the switch flow table. There are a number of applications which are proposed to effectively overcome the DoS attacks. Avant-Guard, Vave and many applications which address the denial of service (DoS) attacks. Avant-Guard addressing the DoS attacks proposes to limit the flow request sent to the control tier. It acts in between the control and the data tier in Software Defined Networking Architecture. Avant-Guard uses a connection migration tool which minimizes the flow of TCP sessions which are failed in the data tier in to the control tier. This reduces the DoS attacks by restricting only the data flow requests which perform a complete TCP handshake (Scott-Hayward, 2015) (OKAMURA, September 2013). Vave is Virtual source Address Validation Edge, an application which is an enhancement of source address validation Improvements (SAVI). Even though, DoS attacks are not directly addressed by Vave, it works on IP Spoofing which would lead the network to a DoS attack. The key factor of Vave is its agility which in turn reduces the packet process overhead and the resource requirement (Scott-Hayward, 2015) (Ye Wang, 2013). There are various applications which address the DoS attacks similar to Avant-Guard and Vave. Distributed Denial of Service Attacks is also one of the highest alert level attacks in a Software Defined Networking Architecture. DDoS attacks are traced using the traffic flow in the network using various algorithms like Naive Bayes, K-Nearest neighbour, K-means, K-medoids to trace the data traffic into the network. These algorithms are used to determine the normal and abnormal traffic based on the detection rate and the efficiency. Additionally using Signature based IDS the anonymous behavior of the host is identified and the alert is raised (Seugwon Shin, 2013).

Unauthorized access in a Software Defined Networking Architecture poses high level of threat as it could completely collapse the network. The possibility of unauthorized access might happen either in the controller or in the API’s running over the controller. AuthFlow, SE-Floodlight, OperationCheckpoint, PermOF, Authentication for Resilience, Securing Distributed Control, Byzantine-Resilient (H. Li, 2014) SDN are few applications addressing the unauthorized access in Software Defined Networking (Scott-Hayward, 2015). AuthFlow - the application uses host credentials for authentication and access control mechanism. The AuthFlow works on the OpenFlow network using the host authentication in the MAC layer or a credential based authentication to ensure a low overhead and fine grained access control (P. Porras, 2012). Unless valid credentials are provided by the host, the access of host is denied in the AuthFlow mechanism (Guang Yao, 2011). Byzantine-Resilient SDN is another application which works on the multiple controllers unlike the traditional single controllers resisting the Byzantine attacks in the controllers (Lohit Barki, 2016).

FortNOX is another security application developed for SDN networks in order to address the Malicious and Compromised applications. The malicious attacks happen via compromised applications sitting over the controllers, in the controllers in the process of exchanging messages. FortNOX implements role based authentication policy in addressing the security issues (Scott-Hayward, 2015) (D. M. F. Mattos).

There are several other applications addressing the security issues possible in the Software Defined Networks. Each application targets the specific type of attack and placed at the possible weak points in the network. Whole together, all the applications addressing the security aspect of the Software Defined Networking needs a trusted connection using trust manager, proper and secure authentication process between source and destination.

V. CONCLUSION AND FUTURE WORK

Software Defined Networking, considered being a dynamic, cost efficient, vendor independent architecture, is in an infant level of deployment, is graphing its growth gradually in a raising mode. There are a lot of issues needed to be addressed in Software Defined Networking. A brief analysis was done in this paper focusing on the existing security features in Software Defined Networking, identifying the possible threats, the weak points and the existing security applications. The study, even though giving a picture of exponential growth in addressing the security issues of SDN Networks, a lot of research work is further required in making a stronger and secured SDN Network. Out of the few issues of security addressed in this study, issues such as Data Leakage and modifications are yet to be addressed in a full-fledged and effective manner. A productive approach is adapted in the entire security application research focusing on key factors such as Authentication, Authorization and Access to the network based on security keys and trust management concept. We could not arrive to a conclusion based on this restrictive analysis in either ways, that SDN networks are secured and stronger or SDN networks are limited in the perspective of security. But, the basic study on security aspects of SDN clearly depicts the requirement of a broader, wider and in-depth growth in all the aspects fortifying from the current and upcoming threats and attacks.

REFERENCES

1. A discussion with Amin Vahdat, D. C. (2016, March). A Purpose-Built Global Network: Google's move to SDN. Communications of the ACM , 59(3), 46-54. doi:DOI:10.1145/2814326
2. D. M. F. Mattos, L. H. (n.d.). AuthFlow: authentication and access control mechanism for software defined networking.
3. Diego Kreutz, F. M. (2013). Towards Secure and Dependable Software-Defined Networks. HotSDN’13. Hong Kong, China.: ACM. doi:978-1-4503-2178-5/13/08
4. Guang Yao, J. B. (2011). Source Address Validation Solution with OpenFlow/NOX Architecture. 2011 19th IEEE International Conference on Network Protocols.
5. H. Li, P. L. (2014). Byzantine-resilient secure software defined networks with multiple controllers. Communications (ICC), IEEE International Conference, 695-700.
6. Jerome Francois, L. D. (2014). Network Security through Software Defined Networking: a Survey. IPTComm'14 . CHICAGO, IL, USA: ACM. doi:http://dx.doi.org/10.1145/2670386.2670390.
7. Kaliyamurthy Nitheesh Murugan, S. T. (2019). Securing the SOHO Software Defined Network with the Extended User Interaction. Journal of Advanced Research in Dynamical and Control Systems, 11(10 Special Issue), 148-151. doi:10.5373/JARDCS/V11SP10/20192785

8. Kannan Govindarajan, K. C. (2013). A literature review on Software-Defined Networking (SDN) research topics, challenges and solutions. Fifth International Conference on Advanced Computing (ICoAC) (pp. 293 - 299). IEEE Conference Publications. doi:10.1109/ICoAC.2013.6921966
9. Kirkpatrick, K. (2013, September). Software-Defined Networking. Communications of the ACM, 56(9), 16-19. doi:10.1145/2500468.2500473
10. Lohit Barki, A. S. (2016). Detection of Distributed Denial of Service Attacks in Software Defined Networks. 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2576-2581). Jaipur, India: IEEE.
11. NetworkSecurity. (n.d.). Retrieved from http://www.networxsecurity.org/: http://www.networxsecurity.org/members-area/glossary/s/sdn.html
12. Nitheesh Murugan K, L. J. (2016). Enhanced Security in Computer Networks based on Multilevel System and User Intervention. DOI: 10.1109/SCOPES.2016.7955575, ISBN: 978-1-5090-4620-1.
13. OKAMURA, O. M. (September 2013). Securing Distributed Control of Software Defined Networks. IJCSNS International Journal of Computer Science and Network Security, 13(9).
14. P. Porras, S. S. (2012). A security enforcement kernel for OpenFlow networks. Proceedings of the first workshop on Hot topics in software defined networks, 121-126.
15. R.L., S. (2014). SDN for network security. IEEE.
16. Raphael Horvath, D. N. (2015). A Literature Review on Challenges and Effects of Software Defined Networking. Conference on ENTERprise Information Systems / International Conference on Project. Elsevier ScienceDirect Procedia Computer Science. doi:10.1016/j.procs.2015.08.563
17. S. Shin, V. Y. (2013). AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks. ACM SIGSAC Conference on Computer & Communications Security (pp. 413-424). Berlin, Germany: ACM. doi:http://dx.doi.org/10.1145/2508859.2516684.
18. Scott-Hayward, S. N. (2015). A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials, 18(1), 623-654. doi:10.1109/COMST.2015.2453114
19. Seugwon Shin, P. P. (2013). FRESCO: Modular Composable Security Services for Software-Defined Networks. ISOC Network and Distributed System Security Symposium.
20. Seungwon Shin, G. G. (2013). Attacking Software-Defined Networks:A First Feasibility Study. HotSDN'13. Hong Kong, China.: ACM. doi:978-1-4503-2178-5/13/08.
21. Seungwon Shin, L. X. (2016). Enhancing Network Security through Software Defined Networking (SDN). 25th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-9). IEEE Conference Publications. doi:DOI:10.1109/ICCCN.2016. 7568520
22. Wenfeng Xia, Y. W. (2015). A Survey on Software-Defined Networking. IEEE Communications Surveys & Tutorials, 17(1), 27 - 51. doi:10.1109/COMST.2014.2330903
23. Ye Wang, Y. Z. (2013). NetFuse: Short-circuiting Traffic Surges in the Cloud. IEEE International Conference on Communications (ICC), 3514 - 3518. doi:10.1109/ICC.2013.6655095.