International Journal of Computer Applications Technology and Research
Volume 7–Issue 08, 297-300, 2018, ISSN:-2319–8656

Security in Software Defined Networks (SDN): Challenges and Research Opportunities for Nigeria.

Abdulsalam S. Mustafa
Khazar University
Baku, Azerbaijan.

Donald Mkpanam
National Institute for Legislative and Democratic Studies, National Assembly
Abuja, Nigeria.

Ali Abdullahi
National Institute for Legislative and Democratic Studies, National Assembly
Abuja, Nigeria.

Abstract: In networks, the rapidly changing traffic patterns of search engines, Internet of Things (IoT) devices, Big Data and data centers has thrown up new challenges for legacy; existing networks; and prompted the need for a more intelligent and innovative way to dynamically manage traffic and allocate limited network resources. Software Defined Network (SDN) which decouples the control plane from the data plane through network vitalizations aims to address these challenges. This paper has explored the SDN architecture and its implementation with the OpenFlow protocol. It has also assessed some of its benefits over traditional network architectures, security concerns and how it can be addressed in future research and related works in emerging economies such as Nigeria.

Keywords: SDN; OpenFlow; Mobile Networks; Network Security; IoT; Big Data

1. INTRODUCTION

1.1 Background

Software Defined Networking (SDN) decouples the control plane from the data plane in order to enhance programmability and flexibility of the control and management of a network. Legacy networks are regarded as complex and rigid, difficult to scale and manage, and too costly but SDN provides a more innovative and dynamic network architecture that transforms traditional network architecture into rich service-delivery platforms [1]. SDN, places a layer of software over the network like a network operating system which interacts with all routers in the network. A major outcome of its design and development is its inherent security and simplified networking. Its emergence offers a robust environment for designing future networks that will be dynamic, cost effective, adaptable, and flexible, and suitable for high bandwidth use and dynamic nature of present applications [2].

The Architecture and Framework working group proposed a Software Defined Network model composed of the application plane, the controller plane and the data plane [3]. SDN developers aim to achieve scalability and agility in network management through separation of the control plane (the controller) which decides where packets are sent from the data plane (the physical network) which forwards traffic to its destination [3]. SDN increasingly uses elastic cloud architectures and dynamic resource allocation in its infrastructure goals [4]. SDN forwarding decisions are flow based in comparison to destination based traditional networks. Openflow was the most commonly used SDN protocol and presently, most companies have decided to adopt different protocols. Some of the protocols currently used are open network environment by Cisco and network virtualization platform by Nicira [3]. This paper's objective is to identify some of the challenges and research opportunities for SDN implementation in Nigeria. Some of the applications of SDN include data center, wide area backbone networks, enterprise networks, internet exchange points and home networks.

Figure 1 below consists of the 3 distinct layers: application layer; control layer; and infrastructure or physical layer.

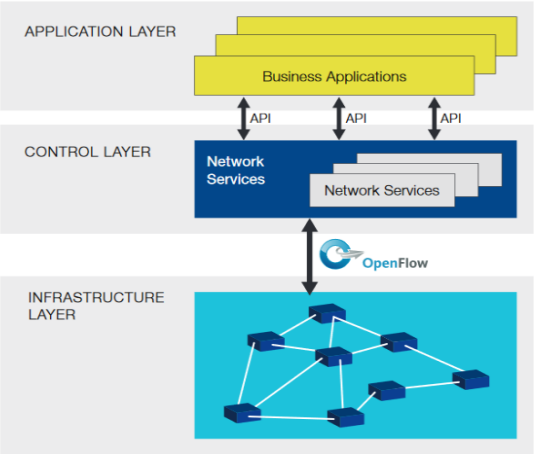

Figure 1. SDN Architecture [3]

1.2 Benefits of SDN

The separation of the control and data planes increases the flexibility of the network to adapt to evolving networks. One of the major benefits for operators and service providers is reduction in operation cost due to centralized management, efficiency in operations and existing hardware being fully utilized. The ability of the networking infrastructure to be programmable and manageable makes it scalable and more dynamic. Other expected benefits include increased network reliability and security discussed in this paper in addition to better user-experience due to SDN ability to adapt to dynamic user-needs. SDN is also expected to manage inflow of traffic from internet of things (IoT) devices by segmenting the traffic and helping to orgainse the data. Furthermore, SDN is expected to enable networks keep pace with the speed of

change on a network without the need to continuously invest in new infrastructure or devices.

1.3 SDN and Mobile Networks

OpenFlow-based SDN offers several benefits for mobile networks, including wireless access segments, mobile backhaul networks, and core networks [5], [6]. SDN will enable carrier networks benefit from its architecture by incorporating innovative ways of managing and controlling the network [5], [6]. In addition, it will increase flexibility by enabling the smooth introduction of new service bundles and value-added services at a faster pace in Nigeria. The future 5G network aims to incorporate SDN principle in its framework and in network slicing concept. A recent position paper by Malik et.al. [5] on SDN based mobile networks suggests that it can simplify mobile networks and lower management costs. Furthermore, SDN in mobile networks is expected to provide maximum flexibility, openness, and programmability to future carriers without the need to make changes in user-equipment. In addition, SDN could provide mobile operators with greater control over their equipment and infrastructure and simplify network management.

2. LITERATURE REVIEW: RELATED WORKS

In a computer network, communication is effected between the network and its host through the use of switches and routers configured for data packet and routing functionality. Configurations on the devices occur through a process of translating high-level network policies into device-specific low-level commands, which is manually done through command-line or graphical user interfaces (GUI) [7]. This is vulnerable to security issues; exploitation; threats and attacks on the network including Denial of Service (DoS) attacks; compromised controller attacks (faulty or hijacked controllers); spoofing attacks; malicious interjection; traffic anomaly; and forwarding control link attacks.

Colville & Spafford [8] reveal, that lack of integrated network control creates network management challenges and the error-prone configuration process triggers network faults, bugs, and security lapses. Feldmann et al. [9] suggest that because of inflexibility, network innovation has essentially stagnated. However, SDN model frontally addresses this challenge by separating the packet forwarding functionality of the forwarding devices or data plane from the control element or control plane [6]. The separation technique which is technically called decoupling remains a key feature of SDN. Decoupling spawns innovative network architecture where the network switches functions such as basic forwarding devices and the control logic is implemented in a logically centralized controller [10].

Akhunzada et.al. [11], argue that the integrity and security of SDNs remain unproven regarding the placement of management functionality in a single centralized virtual server making it easier to compromise the whole network through a single point of failure. However, Medhi et.al. [12], claim that SDN provides a unique opportunity for effectively detecting and containing network security problems in home and office networks. The research findings of Medhi et.al. [12], reveal four prominent track anomaly detection algorithms which can be implemented in an SDN framework using Open flow compliant switches and NOX (open source development platform for C++ based SDN control applications) as a controller. They further indicated that these algorithms are significantly more accurate in detecting malicious activities in the home networks in comparison to the Internet Service Provider (ISP) [12].

SDN's major security issue is being self-secure. Kreutz et.al. [6] advocated incorporating security and dependability into the SDN architecture from the ground level up. According to them, SDN is susceptible to several threats such as forged traffic flow to attacking network entities; Denial of Service (DoS) attacks on switches, controllers and control plane communications [13]. Potential attacks on the interface between the controller and high-level applications, exploiting the weaknesses in Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocol implementations in addition to switches in the network may be hijacked or exploited [14]. These are missing gaps that this study will attempt to address on the security issues in the evolution of SDN and its adoption by service providers in Nigeria.

Kreutz et.al. [15] proposed stringent authentication mechanisms and trust models which could counter common identity-based attacks as few of the potential solutions to the identified threats inherent in the current SDN is a monotony-regime [16]. Therefore, there is need to diversify the protocols, controllers, and tools employed and consequently reduce common implementation vulnerabilities, a major focus of this study. Shin et.al. [17] propose FRESCO, a security-specific application development framework for OpenFlow networks for securing the design of SDN. FRESCO simplifies transferring of the application programming interface (API) scripts to enabling the development of threat-detection logic and security monitoring as programming libraries [17].But Akhunzada et.al. [11] state that, FRESCO does not improve the security of the application and infrastructure layers of SDN.

As alternatives, Shirali-Shahrez and Ganjali [18], propose FleXam, a sampling extension for OpenFlow to enhance the security of SDN while Shing and Gu [16], propose CloudWatcher, a framework for monitoring clouds. Kreutz et.al. [13] propose L-IDS, a learning intrusion detection system to protect mobile devices in a specific location which they regard as a prominent solution for security enhancement. Also, Wang et.al. [19] offer a systematic approach to detecting and resolving conflicts in an SDN firewall by checking firewall authorization space and flow space using 'header space analyses' to investigating the effectiveness and efficiency of this approach in addressing security analyses threats.

Shin et.al. [17] suggest the use of connection migration, an extension to the data panel to reducing interactions between data and control panel to addressing DoS attacks on the southbound interface. This is like the approach proposed by Ying-Dare et. al. [20], for reducing the traffic overhead to the controller and providing NFV through an extended SDN architecture. Their evaluation show that in the extended SDN architecture, only 0.12 percent of the input traffic is handled by the controller extended, while 77.23 percent is handled on the controller in conventional architecture [20]. Akhunzada et. al. [11] also claim that, OpenWatch, an adaptive method of flow counting to detect anomalies in SDN is a credible solution for security analyses and is expected to improve the overall security of Network protocols such as OpenFlow. Ali et al. [7] points out, that as cyber-threats continue to evolve and become more sophisticated, the potentials of a highly configurable network attack is catastrophic, hence, the need to move away from the reactive strategy approach common to

legacy networks. It is evident that there a lot of vulnerabilities which could target SDN. This study will address security threats to the configuration of SDN so as make it suitable for large scale adoption and deployment in Nigeria.

3. DISCUSSIONS AND FUTURE RESEARCH

As SDN is being adopted, there is demand for secured SDN solutions and a more adaptable secured framework. Several issues relating to SDN are currently actively being researched, however, there is also need for security vulnerability assessment because this is an important process that must be conducted to fully secure a system before its deployment. The Control plane in SDN handles configuration management of devices, responsible for routing decisions and monitoring the network. The controller is considered as a single point of failure [15], and it is a major security target. In this regard, there is need to investigate new security architectures for the controller to support more innovative security services and intelligent network defense systems.

FRESCO by Shin et.al. [17], is an extension of the research work done by Kreutz et.al. [15], which that makes it easy to make and deploy security services in SDN, however, they believe none of those works adopts or enforces the security of SDN itself [15]. Furthermore, there is need for research on creating more secured and resilient SDN controllers and approaches to addressing the security issues. This therefore generates the normative question of how innovative SDN-based security applications can potentially replace existing security applications? There is also the question of how new vulnerabilities in SDN controllers can be exploited through threat vectors and possible solutions and improvements to address these problems? In addition, there is the need to question the handling of malicious applications being developed and deployed on SDN controllers?

4. CONCLUSIONS

In this paper, we have discussed the concept of Software Defined Network framework which uses network virtualization to separate the control plane from the data plane. With a centralized control, SDN can easily manage and enable networks to adapt and cope with unpredictable traffic patterns which can place high demands on the limited network resources. However, in any network, security is a major concern, therefore, it is imperative to do an analysis of security challenges in SDN from the perspective of attacks on SDN controllers and development of a new mitigation technique and security model. To achieve this requires further research, data gathering, testing, consultations with specialists in this area and do more feasibility studies. The result of future research will provide more innovative methods for threat management and mitigation of attacks on SDN controllers while enhancing overall network security and management. This will support more secured networks and drive the adoption of SDN which is considered more cost effective and will be beneficial to emerging economies such as Nigeria.

5. ACKNOWLEDGMENTS

The authors would like to thank Khazar University and NILDS NASS for their support.

6. REFERENCES

[1] Liu, S., and Li, B. 2015. On Scaling Software-Defined Network in Wide-Area Networks. Tsinghua Since and Technology. 20(3). 221-232.

[2] Open Network Foundation 2015. Principles and Practices for Securing Software-Defined Networks. ONF TR-511.

[3] Anthony, L. 2015. Security Risks in SDN and Other New Software Issues. RSA Conference. Frost and Sullivan.

[4] Malik, M.S., Montanari, M., Huh, J.H., Bobba, R.B., and Campbell, R.H. 2013. Towards SDN enabled network control delegation in clouds. 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

[5] Open Network Foundation (ONF). 2013. SDN Architecture Overview.

[6] Ali, S.T., Sivaraman, V., Radford, A., and Jha, S. 2013. A Survey of Securing Networks Using Software Defined Networking. IEEE Transactions on Reliability. 3(64).

[7] Colville, J., and Spafford, G. 2010. Configuration Management for Virtual and Cloud Infrastructures. Gartner Inc.

[8] Feldmann, A., Kind, M., Maennel, O., Schaffrath, G., and Werle, C. 2013. Network Virtualization - An Enabler for Overcoming Ossification. Future Internet Technology. European Community in Information Technology (ERCIM) News.

[9] Open Network Foundation. 2013. OpenFlow-Enabled Mobile and Wireless Networks. ONF Solution Brief.

[10] Akhunzada, A., Ahmed, E., Gani, A., Khan, M.K., Imran, I. and Guizani, S. 2015. Security and Privacy in Emerging Networks: Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues. IEEE Communications Magazine. 34-44.

[11] Mehdi, S.A., Khalid, J., and Khayam, S.A. 2011. Revisiting traffic anomaly detection using software defined networking. In Proceedings of 14th Int. Symposium on Recent Advances in Intrusion Detection (RAID). 6961. 161–180.

[12] Kreutz, D., Ramos, F.M.V., and Verissimo, P. 2013. Software-Defined Networking: A Comprehensive Survey. In Proceedings of the IEEE,103(1). 55-60.

[13] Dabbagh, M., Hamdaoui, B., Guizani, M., and Rayes, A. 2015. Software-Defined Networking Security: Pros and Cons. IEEE Communications Magazine, Communications Standards Supplement.

[14] Kreutz, D., Ramos, F.M.V., and Verissimo, P. 2013. Towards secure and dependable software defined networks, In Proceedings of the second ACM SIGCOMM Workshop on Hot topics in software defined networking. ACM, 55–60.

[15] Shin, S., and Gu, G. 2013. CloudWatcher: network security monitoring using OpenFlow in dynamic cloud networks. Springer. 92–103.

[16] Shin, S., Yegneswaran, V., Porras, P.A., and Gu, G. 2013. AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks, In Proceedings of 2013 ACM SIGSAC Conference on Computer and Communications Security. 413–424.

[17] Shirali-Shahrez, S., and Ganjali, Y. 2013. FleXam: Flexible Sampling Extension for Monitoring and Security Applications in OpenFlow. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. HotSDN'13. 167-168.

[18] Wang, Y., Wen, X., Chen, Y., Hu, C., and Shi, C. 2013. Towards a Secure Controller Platform for Openflow Applications, Proc. 2nd ACM SIGCOMM Workshop on Hot topics in Software Defined Networking, 171–72.

[19] Ying-Dar, L., Po-Ching, L., Chin-Hung, Y., Yao-Chun, W., and Yuan-Cheng, L. 2015. An Extended SDN Architecture for Network Function Virtualization with a Case Study on Intrusion Prevention, IEEE Network.

[20] Li, Y. 2014. Computer Networks 72. 74–98.

[21] Metzler, J. 2012, Understanding Software-Defined Networks, Information Week Reports. 1–25.

[22] Scott-Hayward, S., Natarajan, S., and Seker, S. 2016. A Survey of Security in Software Defined Networks. IEEE Communication Surveys and Tutorials. 18(1).

[23] Shin, S., Porras, P., Yegneswaran, V., Fong, M., Gu, G., and Tyson, M. 2013. FRESCO: Modular Composable Security Services for Software-Defined Networks. IOSC Network and Distributed System Security Symposium (NDSS).

[24] Anon. 2016. Software-Defined Networking (SDN) Definition. [online] Available at: http://www.opennetworking.org. [Accessed 5 Mar. 2007].

[25] Son, S., Shin, S., Yegneswaran, V., Porras, P.A., and Gu, G. 2013. Model Checking Invariant Security Properties in OpenFlow. In Proceedings of IEEE ICC. 74–79.