*https://dx.doi.org/10.24001/ijaems.3.5.18* *ISSN: 2454-1311*

# The Impact on Security due to the Vulnerabilities Existing in the network a Strategic Approach towards Security

Dr. Swapnesh Taterh

Associate Professor, Amity Institute of Information and Technology, Jaipur, India
staterh@jpr.amity.edu

***Abstract—*** *Software Defined Networking, the emerging technology is taking the network sector to a new variant. Networking sector completely focused on hardware infrastructure is now moving towards software programming. Due to an exponential growth in the number of user and the amount of information over wires, there arises a great risk with the existing IP Network architecture. Software Defined Networking paves a platform identifying a feasible solution to the problem by virtualization. Software Defined Networking provides a viable path in virtualization and managing the network resources in an "On Demand Manner". This study is focused on the drawbacks of the existing technology and a fine grained introduction to Software Defined Networking. Further adding to the above topic, this study also passes over the current steps taken in the industrial sector in implementing Software Defined Networking.*

*This study makes a walkthrough about the security features of Software Defined Networking, its advantages, limitations and further scope in identifying the loopholes in the security.*

***Keywords— Software Defined Networking (SDN), Quality of Service (QoS), Transmission Control Protocol/ Internet Protocol (TCP/IP), Open Network Foundation (ONF), Control Plane, Data Plane, Spoofing, Distributed Denial of Service (DDoS), Tampering, Centralized Controllers, Intrusion Prevention.***

## I. INTRODUCTION

Software Defined Networking, one of the emerging trends in the field of Networking, is focused by a whole lot of researchers in analyzing its potential operations and viable security aspects to make a successful implementation in the existing network architecture. Software Defined Networking is really a cost and complexity impact technology to be adopted in the near future(Dutta, 1998).

The main focus of Software Defined Networking is to drastically reduce the cost of investments done in physical network devices and to increase the potential controls and functions of a Network Infrastructure in an easier and efficient manner. Software Defined Networking is a one point control, otherwise a Centralized Control which has a wider visibility of the entire network for which it is designated(Seungwon Shin, 2016).

The architecture of Software Defined Networking is designed to provide programmability for a network(Wenfeng Xia, 2015). The critical challenges focused in the existing network systems since they have evolved are not limited to the size of the network, the bandwidth speed and the security. Right from the day of evolution of networks, the research in addressing the above challenges was also in a run. The result of researches in-turn was made as the growth of technology starting from LAN, WAN Switching with a bandwidth speed 1 Mbps ranging now with a high speed 100 Gbps. At the time, the higher bandwidths implemented, trying to resolve the speed problem in a network, the other technological growth also were indexing to resolve the issues related to safer handling of data in a network with various latency techniques, QoS, Load balancing Algorithms, Build-in Security Policies and much more. These progressive changes happening all around the past 30 years have given a hand to the researchers to take the networking domain into a new variant. The utilization of Cloud Computing in huge data centers(Wenfeng Xia, 2015), seeing a lot of advantages in the case of efficient computing resources, leverages the researchers to provide a centralized networking facility/ architecture(Kannan Govindarajan, 2013).

This paper focuses on the security aspects of the emerging centralized networking technology, the Software Defined Networking. This work is structured the following way: Part II will talk about the existing Network Infrastructure, Part

*https://dx.doi.org/10.24001/ijaems.3.5.18* *ISSN: 2454-1311*

III will talk briefly about Software Defined Networking, its History, its Architecture, its advantages and its features, Part IV will talk about the Industry's perspective and view on Software Defined Networking and their need to concentrate on Software Defined Networking, Part V will focus on the Security features available in Software Defined Networking, Part VI will focus on the limitations and Part VII will talk about the possible future work in enhancing the security features of SDN. This entire work is designed in such a way that it provides a broader view to all new researchers on Software Defined Networking to understand the whole scenario about Software Defined Networking and its challenges. On completion of this work, it will give a precise idea about the security features of Software Defined Networking in the real time environment.

## II. EXISTING NETWORK SCENARIO

The existing network infrastructure, the IP based Network known as Transmission Control Protocol (TCP) and the Internet Protocol (IP). These protocols are based onthe TCP/IP standards which are widely used in network communications (Ameen Banjar, 2015).The Internet, being a practical existence in all day to day activities, the communications between networks are more heavier which raises the risk of increasing "performance" bottlenecks (Hailong Zhang, 2015). The architecture of TCP/ IP is designed in such a way that it makes better utilization of all the resources available and focus on all the specification of data starting from data formats, its transmission, addressing, routing till the data being received at the destination. This enables the existing standards to allow high throughput in the networks (Ameen Banjar, 2015).

The physical routing device, whichever receives the data in the form of packets does two things. It identifies the network flow (network map) and forwards the data packets to the destination based on protocols and algorithms as configured in the device. The rapid increase in the number of users and the range of cloud applications brings out a hard situation in handling the data with regard to its performance and its convergence time. Automatic reconfiguration and other response mechanisms have no concentration in the existing standards(Diego Kreutz, 2015).

In the case of larger network size and during the increase of delay or bandwidth in a network, the potentiality of IP Networking is a big Question (Andreas R. Urke, 2012). The exhaustion of IPv4 addresses also makes the situation further tougherto step up with a solution for the arising problem. Further delaying in finding out appropriate solution and migrate from the existing scenarios will lead to a whole lot of fuss in the Network domain(Loshin, 2004). The unavailability of 32 bit IP Addressing (IPv4) forced to move towards 128 bit IP Addressing (IPv6) which is now a relief towards the unavailability of unique id problem. However, to migrate from 32 bit to 128 bit is not practically possible with in a fraction of second with existing network infrastructures probably not manufactured to adopt this transition (Oppenheimer, 2012).

To come up with a feasible solution to handle this problem, the focus has to be funneled down from addressing the problem in the perspective of unique identification of devices into hardware and software implementation. The focus now laid on the physical routing devices, the hardware part, which is working on two functions, creating the network map and forwarding the data packets. Working on the network map is done by the control plane based on protocols like Open Shortest Path First Protocol, Border Gateway Protocol, Routing Information Protocol and various proprietary protocols. The forwarding of data packets is done by the data plane based on the decision taken by the control plane(Perlman, 1999). The operations of both Control and Data Planes occur in the same physical device which will be more complicated while implementing IPv6 Addressing. This potentially leads the routing tables to be large, thereby reducing the efficiency of the physical devices. This raises the need of bifurcation of data and control operation in physical devices(Danielkleviansky).

## III. SOFTWARE DEFINED NETWORKING

The challenges faced in the existing network infrastructure paves way to the researchers to unleash their ideas in the field to come up with optimal and feasible solution to the existing problem. Software Defined Networking, the faster growing trends in the field of Networking, paves a better platform in addressing the existing issues.

The Software Defined Networking, even though considered as an emerging new technology, it emerged from various concepts which are derived in the past years. Few games like Websproket, War Room, Krieg spiel(kriegsspiel) were denoting the basic concepts of Software Defined Networking. However, it does not mean that Software Defined Networking was introduced in the 18$^{th}$ century.

In the year 1997, GeoPlex a common IP Software Platform was introduced which acted as a managing network middleware(Dutta, 1998) developed by AT&T. This is an enhanced network infrastructure which is also one of the itching factors to evolve Software Defined Networking.

*https://dx.doi.org/10.24001/ijaems.3.5.18* *ISSN: 2454-1311*

This raised the idea of requiring a soft switch which can provide flexibility in the network.

In 2001, first soft switch was developed by Ericson, known as Supranet Transaction Server. It is a technology which makes the set of instructions to dynamically transmit across the network without any interruption of service to the host ((NetworkSecurity).In 2011, the Open Networking Foundation was formed which is setting standards for Software Defined Networking. Open Flow Standard, Open Flow Configuration and Management are Software Defined Networking Standards which are defined by ONF(Open Networking Foundation).

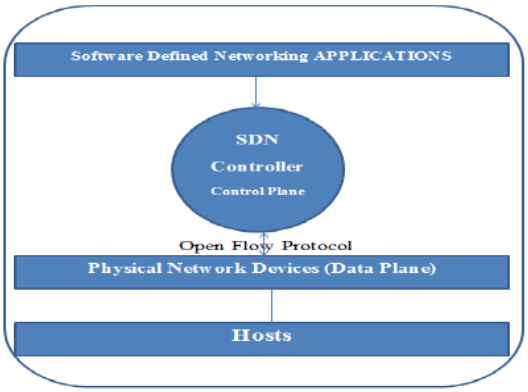


*Fig.1: General SDN Architecture*

Software Defined Networking is designed in such a way it decouples the data and control plane enabling to break the network control into manageable sectors. The control plane, works on mapping the network has a centralized control over the network with the help of software components through a server and the data plane works on forwarding the data packets is on the physical network devices thus enabling flexibility, scalability, security, quality and bandwidth based on the network requirements. Software Defined Networking is a technology which helps in virtualization of physical network devices based on "On Demand" requirements. (Kannan Govindarajan, 2013).

The main focus of Software Defined Networking is to reduce the problems raised in the existing IP Networking Architecture. The SDN Architecture removes the controlplane from the physical networking device which in-turn will reduce the high complication in those devices due to high throughput. Unlike the existing architecture, since the control plane is not in the physical network devices, the forwardingdecisions are flow based and not destination based. This enables a high level of flexibility in rendering data transmission as per the requirement of the end users. The control plane, which is made as a software platform, is not in the physical networking devices, providing logically centralized view on the network (Diego Kreutz, 2015).

The Software Defined Networking is a three layered architecture.

*Table.1: Three Layered Architecture –Software Defined Networking*

| ***Controller(NB)*** | ***Application*** | ***Objective*** | ***Protocol (SB)*** |
|---|---|---|---|
| ***NOX*** | *Elastic Tree* | *Energy aware routing* | *Open Flow* |
| | *Aster*x* | *Load Balancing* | |
| | *OSP* | *Fast Recovery* | |
| ***POX*** | *FlowQoS* | *QoS for Broadband* | |
| | *OpenNetMon* | *Monitoring QoS Parameters* | |
| ***FloodLight*** | *PolicyCop* | *QoS policy management framework* | |
| | *QoS for SDN* | *QoS over heterogeneous network* | |
| | *LIME* | *Live network migration* | |
| ***FlowVisor*** | *FlowDiff* | *Detects Operational Problems* | |
| | *OpenRoads* | *Control Data path* | |

The data plane which are the physical networking devices, controlled by the control plane through various protocols. The management plane is the software platform which is helpful to control the entire network flow. Software Defined Networking focuses on Dynamic Flow Control, Network wide visibility with Centralized Control, Network Programmability and Simplified Data Plane. A network application program (management plane) will be controlling the data planes in Software Defined Networking(Seungwon Shin, 2016).There are different controllers available in which few are listed in the Table 2(Diego Kreutz, 2015).

*https://dx.doi.org/10.24001/ijaems.3.5.18* *ISSN: 2454-1311*

* NB: North Bound; SB: South Bound

*Table.2: Controllers in SDN and its objective (North and South Bound)*

| ***Management Plane*** | ***Control Plane*** | ***Data Plane*** |
|---|---|---|
| ***User Interface – Authorization*** | *Device Control – Routing* | *Physical Infrastructure* |
| ***System Administration – Accounting*** | *Network Discovery – BGP* | *Switching Fabric* |
| ***Authentication – Logs*** | *Network Mapping – OSPF* | |

The physical networking devices in SDN will act as only a forwarding device and the other where and how part will be done by the Control Plane(Kannan Govindarajan, 2013).

## IV. SECURITY FEATURES IN SOFTWARE DEFINED NETWORKING

Software Defined Networking provides flexible, scalable, programmable and automated network resources within a network. These feasibilities raise a big question on the network's Quality of Service, Security, Load balancing and many other aspects. SDN is used to provide security in the network by improving the security itself (Diego Kreutz, 2015). While all the aspects are now in the hands of researchers to come up with feasible solutions, Security is taken as one of the prime factor in enhancing and deploying Software Defined Networking, as the networks implementing SDN Architecture would be dealing with enormous amount of information.Software Defined Networkinghas the potential to secure its network without using any additional infrastructure by using its own software applications (Seungwon Shin, 2016).

Considering security in an SDN Architecture, the main focus is to secure the SDN Controller, the intelligent device in the model controlling the data plane. Distributed Denial of Service Attacks, Intrusion Prevention, Spoofing, Tampering, Repudiation, Information Disclosure and Elevation of Privilege(Asoke K. Talukder, 2009)are the other areas which have to be concentrated in implementing security. On a security aspect, Software Defined Networking has an upper hand in deducting and reacting to DDoS attacks because of its software-based traffic analysis methods, centralized control, global view of the network and dynamic updating of forwarding rules(Yan, Yu, Gong, & Li, 2016).

There are few countable mechanisms like NetFuse and Fresco which deals with Security(Kannan Govindarajan, 2013). NetFuse, a scalable mechanism proposed by Ye Wang et al. in 2013 focus on factors like Distributed Denial of Service Attacks, routing misconfigurations, operator errors and workload changes. It resides in between OpenFlow Controllers and the switches using toxin – antitoxin like mechanism (Ye Wang, 2013). It uses a Flow Aggregation Mechanism and NP – Hard Combinational Optimization Algorithm implementing flow redirection, delay injection and packet blocking, which improves the scalability of the network (Kannan Govindarajan, 2013). Active Security is another security mechanism which works in a Floodlight Controller based to on protection, sense, adjust, collect and counter(Diego Kreutz, 2015).

Fresco, is an OpenFlow security application development framework developed in the year 2013 works on NOX Controller. It works based on the input, output, parameter, action and events factor. DROP, REDIRECT and QUARANTINE are the security policies which are enforced by the framework based on the threats(Seugwon Shin, 2013). There are few other security based applications namely Avant-Guard, SDN-RTBH, CloudWatcher, DDoS detection, SANE, VAVE etc which work on various controllers like Floodlight, POX, NOX.

## V. FUTURE WORK

Software Defined Networking needs to focus on many problems like QoS, Latency, Load Balancing and Security, since the architecture is dealing with enormous amount of information in it. Security will be playing a vital role in this domain, since improved security will boost the performance of the network eventually. On addressing the issues related to security, DDoS attacks will be in the limelight. Further research work will need to address the DDoS attacks, the ways to mitigate from the attacks and come out with new approach in avoiding them (Yan, Yu, Gong, & Li, 2016).

## 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] Ameen Banjar, P. P. (2015). Comparison of TCP/IP Routing Versus OpenFlow Table and Implementation of Intelligent Computational Model to Provide Autonomous Behavior. In Z. C. Grzegorz Borowik (Ed.), *Computational Intelligence and Efficiency in Engineering Systems, Part II* (Vol. 595, pp. 121-142).

*https://dx.doi.org/10.24001/ijaems.3.5.18* *ISSN: 2454-1311*

Springer International Publishing. doi:10.1007/978-3-319-15720-7_9

[3] Andreas R. Urke, L. E. (2012). TCP challenges in hybrid military satellite networks; measurements and comparison. *MILCOM 2012 - 2012 IEEE Military Communications Conference* (pp. 1-6). IEEE Conference Publications. doi:10.1109/MILCOM.2012.6415561

[4] Asoke K. Talukder, V. K. (2009). Security-aware Software Development Life Cycle (SaSDLC) - Processes and tools. *IFIP International Conference on Wireless and Optical Communications Networks* (pp. 1-5). IEEE Conference Publications. doi:10.1109/WOCN.2009.5010550

[5] Danielkleviansky. (n.d.). *http://danielkleviansky.com/separation-of-control-plane-and-data-plane-in-performance-networks/*. Retrieved from http://danielkleviansky.com: http://danielkleviansky.com/separation-of-control-plane-and-data-plane-in-performance-networks/

[6] Diego Kreutz, F. M. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE, 103*(1), 14-76. doi:10.1109/JPROC.2014.2371999

[7] Dutta, P. (1998). Internet object caching. *Intelligent Network Workshop,Proceedings of 7th IEEE* (pp. 95 - 118). 1998 IEEE Conference Publications. doi:10.1109/INW.1998.713263

[8] Hailong Zhang, J. Y. (2015). Performance of SDN Routing in Comparison with Legacy Routing Protocols. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 491 - 494). IEEE Conference Publications. doi:10.1109/CyberC.2015.30

[9] 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

[10] *kriegsspiel*. (n.d.). Retrieved from http://www.kriegsspiel.org.uk: http://www.kriegsspiel.org.uk/index.php/articles/origins-history-of-kriegsspiel/3-origins-of-the-kriegsspiel

[11] Loshin, P. (2004). *IPv6: Theory, Protocol, and Practice* (Vol. 2nd Edition). Morgan Kaufmann Publishers.

[12] Ma, C. (2014). *SDN secrets of Amazon and Google*. Retrieved from http://www.infoworld.com: http://www.infoworld.com/article/2608106/sdn/sdn-secrets-of-amazon-and-google.html?page=2

[13] *NetworkSecurity*. (n.d.). Retrieved from http://www.networxsecurity.org/: http://www.networxsecurity.org/members-area/glossary/s/sdn.html

[14] *Open Networking Foundation*. (n.d.). Retrieved from https://www.opennetworking.org: https://www.opennetworking.org/about/onf-overview

[15] Oppenheimer, P. (2012). *Top-Down Network Design* (Vol. 3rd Edition). Indianapolis: Cisco Press.

[16] Paul Göransson, C. B. (2014). *Software Defined Network, A Comprehensive Approach* (1 ed.). Morgan Kaufmann.

[17] Perlman, R. (1999). *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols* (Vol. 2nd Edition). Addison-Wesley Professional.

[18] Seugwon Shin, P. P. (2013). FRESCO: Modular Composable Security Services for Software-Defined Networks. *ISOC Network and Distributed System Security Symposium.*

[19] 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

[20] 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

[21] Jaiswal, M. (2014). IP Security architecture, application, associated database, and mode. *International Journal Of Research And Analytical Reviews (IJRAR), 1*(1), 446-453.

[22] Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys &Tutorials, 18*(1), 602-622. doi:10.1109/COMST.2015.2487361

[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