IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207053 |

A Study to Identify the Need of Security in Software-Defined Networks

Sayyed Johar [1], Namitha M V [2]

Assistant Professor, Department of Computer Engineering, JNN College of Engineering, Shivamogga, India[1]

Assistant Professor, Department of Computer Engineering, JNN College of Engineering, Shivamogga, India[2]

ABSTRACT: Software-Defined Networking (SDN) is an emerging architecture which allows flexible management of network. It provides programmable interface to control plane and as well as allows for network virtualization. The SDN technology consists of three parts: flow tables installed on switches, a controller and an OpenFlow protocol for the controller to communicate securely with switches. Software defined network has lot of advantages when compared to traditional networking architectures. Analysing, understanding security strategies of SDN are expected to result in developing a security framework for SDN which would strengthen the growth of SDN as powerful network architecture in all aspects.

KEYWORDS: control plane, Network virtualization, security strategies, flow tables, OpenFlow protocol.

I. INTRODUCTION

In Traditional Computer Networks, Network layer (Internet layer in TCP/IP) is responsible for both routing and forwarding packets. The process of routing is related to building the forwarding tables which is used by forwarding process to forward packets from one interface to another. The routing process activity belongs to control plane whereas forwarding of packets belongs to data plane. Control plane is a decision maker (responsible for routing). The concept of decoupling data plane and control plane was proposed by Martin Casado, Stanford University [11] in 2005. Now this concept has grown to be a most promising networking technology ushering the era of Software Defined Network. Software-Defined Networking (SDN) is an emerging architecture which allows flexible management of network. It provides programmable interface to control plane and as well as allows for network virtualization.This separation of control plane from data plane has enabled the former to be implemented outside the traditional router hardware. This in turns implies that a protocol is needed between control plane software and the router box so that control plane can inform the packet forwarding hardware to update its forwarding tables. The OpenFlow™ protocol fulfills this need and is a foundational element for building SDN solutions [7]. OpenFlow is a programmable network protocol designed to manage and enable inter operation among routers and switches from various vendors. It separates the programming of routers and switches from underlying hardware.

The SDN technology consists of three parts: flow tables installed on switches, a controller and an OpenFlow protocol for the controller to communicate securely with switches. Flow tables (so far known as forwarding tables) are set up on switches. Controllers communicate to the switches via OpenFlow protocol and enable implementation of policies on flows. The controller could set up paths through the network meeting specific requirements, such as speed, fewest numbers of hops or reduced latency depending on the requirement of the application [12].

The interface between OpenFlow controller and other components of OpenFlow switch through secured channel are depicted in Figure 1.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207053 |

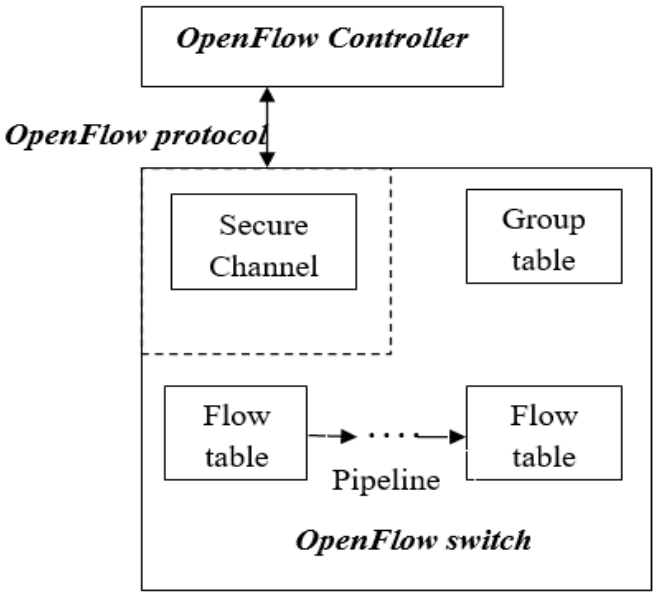

Figure 1: OpenFlow controller and OpenFlow switch interconnection [7].

An OpenFlow Switch consists of one or more flow tables and a group table, which performs packet lookups and forwarding, and an OpenFlow channel to an external controller. The switch communicates with the controller and the controller manages the switch via the OpenFlow protocol.

As the diagram depicts, OpenFlow controller is playing intelligent role as decision maker for forwarding packets, but the success of any networking technology will mainly depend on the deployment of security strategies against any possible security attacks. Certainly, SDN will give rise to new set of security threats as the approach is different from traditional networks. Hence security concern is highly demanding research area.

Paper is organized as follows. Section II describes related work. Literature survey given in Section III. Finally, Section III presents conclusion and future scope.

II. LITERATURE SURVEY

Software defined networking has roots in previous network control systems such as RCP, 4D, SANE, SDN, Ethane [6]. According to the work [4] SDN has 3 interfaces as shown in Figure 2.

1) Southbound Interface – between programmable control plane and data plane.
2) Northbound Interface – between programmable control plane and applications/services.
3) East-West Interfaces – between control planes.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207053 |

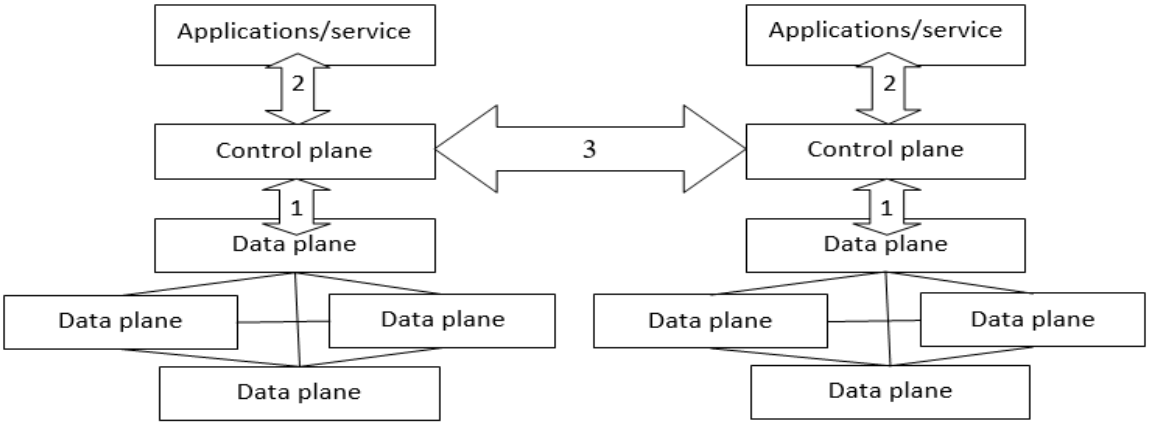

Figure 2: SDN Reference Architecture with south, north, east-west architecture [3][4].

In SDN, the network control plane hardware is separated from the data forwarding plane hardware, i.e., a network switch can forward packets and a separate system can run the network control plane.
Traditional security solutions have primarily focused on static networks with static topology and fixed policies. However, OpenFlow and SDN cannot sustain legacy security strategies, as the approach of OpenFlow and SDN is different compared to traditional networks. With SDN, there's dynamic policy that is under continuous update, where network behavior cannot be predicted. That presents both a challenge and an opportunity for the security community [9].
There needs to be a highly secure controller which checks the authenticity of packets which are coming into it, so that retaining and dropping of packets can be done to avoid unauthorized use of SDN. Controllers should also have a good understanding of security policies required by the organization or application that uses SDN and then provide real-time recognition of violation by any incoming flow. The controller needs to support many OpenFlow applications simultaneously and ensure security. It is highly expected that the controller to protect the network regardless of malfunctioning of applications. [9].
Hence research in the field of SDN, especially identifying security threats, is highly needed; thereby we can realize all the strengths and loopholes of SDN and can find, implement, test and re-implement solutions for the threats found.

III. EXPERIMENTAL RESULTS

We have Discussed the observed vulnerabilities and security threats in the SDN environment. Present quantitative data on the impact of attacks on the network's performance and availability. We have Analyzed the effectiveness of various security mechanisms implemented to mitigate the identified vulnerabilities.

IV. CONCLUSION

Our study justifies software defined radio is having special requirements when compared to traditional networks and hence development of new security strategy is required. Initially it can be done through simulation and emulation. Mininet is a network emulator used to create scalable SDNs using Linux processes. Mininet is used to simulate the topology and test the traffic flows. A Python script is used to create the topology in Mininet, and the traffic flows are received from a remote OpenFlow controller [5]. Later it can be implemented practically. Software defined network has lot of advantages when compared to traditional networking architectures. Analyzing, understanding security strategies of SDN are expected to result in developing a security framework for SDN which would strengthen the growth of SDN as powerful network architecture in all aspects. At the end of the research activity, we may end with significant security strategies, which will make SDN more secured.

V. FUTURE SCOPE

A detailed survey in each component of SDR would be done to identify specific security threats and hence development of security protocols can be considered which suits the requirement.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207053 |

REFERENCES

[1] A practical experience in designing an OpenFlow controller by Roberto Bifulco, Roberto Canonico,Marcus Brunner, Peer Hasselmeyer, Faisal Mir.
[2] Enabling Future Internet Architecture Research and Experimentation by Using Software Defined Networking Fl´avio de Oliveira Silva, Jo˜ao Henrique de Souza Pereira,
Pedro Frosi Rosa, and Sergio Takeo Kofuji.
[3] Improving Network Management with Software Defined Networking. Hyojoon Kim and Nick Feamster, Georgia Institute of Technology.
[4] Software Defined Networking (SDN) :A Reference architecture and open API's. Myung- Ki Shin, Ki-Hyuk Num, Hyoung -Iun Kim.
[5] OpenFlow: Load Balancing in enterprise networks using Floodlight Controller Srinivas Govindraj, Arunkumar Jayaraman, Nitin Khanna, Kaushik Ravi Prakash.
[6] Maestro: Achieving Scalability and Coordination in Centralized Network Control Plane by Zheng Cai, PhD Thesis.
[7] https://www.opennetworking.org/sdn-resources/meet-sdn
[8] http://en.wikipedia.org/wiki/Software-defined_networking
[9] http://www.sdncentral.com/sdn-blog/phil-porras-openflow-secure-controller/2012/07/
[10] https://www.coursera.org/course/sdn
[11] http://en.wikipedia.org/wiki/Software-defined_networking
[12] http://www.networkworld.com/news/2011/041411-open-flow-faq.html

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details