# SECURITY ISSUES IN SOFTWARE DEFINED NETWORKING

Divya Gautam and Shivani Singh
Amity University Madhya Pradesh
Gwalior (M.P)

***Abstract**:* Telecom networks have implemented the fresh concept of the cloud model that is software-defined networking (SDN) to fulfill real time performance and extraordinary obtain ability necessities. The goal of SDN is to convert the mode networks function. SDN and NFV are corresponding technologies; which do not hang on each other. But everything comes with some advantages and disadvantages. Security Defined Networking too has some drawbacks that often put question mark on its abilities. There are various issues regarding the security problems associated with software defined Networking. This Research is focussed on some of the major security issues regarding SDN and will also see some of the best possible solutions which could greatly help us in analyzing SDN.

***Keywords:*** *Software Defined Networks, DoS Attacks, NFV.*

## I. Introduction

Software defined networking is a rising architecture which is active, doable , economical and easy going that makes it perfect for the high bandwidth , driving nature of today's various uses. The security defined architecture uncouples the network control and forwarding functions authorizing network control to be instantly programmable and the hidden infrastructure to be separated for many uses and network services.

The three main sections of security defined networking are:
1. The performance of different tasks for example protocol implementation, firewalls as well as custom policies is the responsibility of Network Management Centre.
2. Control plane condenses control plane intelligence to controller which permits administrator to compose network hardware which belongs to controller. Network is made highly adaptable by this approach.
3. The packets forwarding hardware in the software defined networking architecture is depicted by data plane.

Since ages networking is very known to people. Many network devices are there which are used for some particular tasks for example routers, switches, gateways which are sold by some networking vendors like Cisco and certainly use proprietary hardware. All the tasks of the networking devices are separated by different planes: Control plane, Data plane and Management plane. Control plane exchanges routing information builds ARP table etc. Data plane forwards traffic and relies on data that control plane sends .The management plane can be used for the access as well as the management of the networking devices that is accessing device via telnet ,console port etc. We are following traditional networking since last thirty years and there is nothing wrong in it .But due to various difficult emerging tasks we need more solutions. Security defined networking actually has the solution to it. Traditional networking uses distributed model whereas security defined networking uses central controller for the Control plane. By the help of central controller we can know entire network from one device as it has complete access and information of everything that is happening currently in the network.

The main purpose of Software defined networking is to allow cloud engineers, network engineers and network administrators to reply speedily to mould business necessities by a consolidated control console. Different kinds of network technologies planned to make the network more transparent and light to maintain the virtualized server and storehouse infrastructure of the current data centre are passed by security defined networking.

Wireless networking is though profitable but also has some of its limitations. In wireless networking too security is important. Because anyone who is following same range could easily disturb the respective wireless network. The best thing about SDN is that it provides an opportunity to network administrator so that they could observe unusual activities. They could even compare the present situation with previous situation. Security is an important issue.

## II. Security Issues In Software Defined Network

**SDN Security**

Software defined networking is gaining popularity day by day due to its flexible as well as dynamic approach to networking .But this technology is in its starting days or we can say it is in a childhood stage currently .If a person wants to hack the software or the data etc. then it is obvious that he could go to any extent to do it. He could definitely try to challenge the security of anything latest in the market. Now -a-days software attacks by hackers has become a trend. We know that security could not get enforced by simply laying out the network physically. Even the various operator of security defined networking are not normally security folks. Hence for believing security defined networking we need full trust in the SDN controller as well as the different applications of SDN.

**Security Issues in Networks**

Different from traditional networks, these security issues raise new security requirements on SDN based new network paradigms. Some major issues are:

1. **Network intrusion**: Network intrusion is a major difficulty in traditional networks. These Kinds of networks have disastrous effects over security defined networking. Attackers are now having different techniques of causing network intrusion.

For example: It is very easy for the controllers (who are in continuous communication) to accept forwarding plane. In the same way some third party requests may be related to the controllers pool and due to their unauthorized access, data leakage may occur Due to these issues it is very much necessary to find out network intrusion , firewalls, access control etc.

2. **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** it is among the main security faults in SDN .If this equal to traditional states then in this type of attack is dangerous in security defined networking due to logically centralized control. The storage capacity of present switches could not catch there all forwarding policies. If any switch is not able to discover the incoming packet s matching rule then it will keep the packet into its buffer and for proper routing rule and will suggest query for asking controller. This reactive caching makes controllers and for a denial of service attack it switches susceptibly .Attackers can switch with heavy payload packets which actually belong to diverse flows. In this buffer and switch table upto this duration will be captured fastly. Latest incoming packets will be presented .Temporarily controllers will end its processing power to contract with those queries who initiate cracking in the networking. This attack has acknowledged broad responsiveness in education .various researches have been done to resolve this issue.

3. **Application trust management**: One more problem in security defined networking is how to get different network application from application plane. A programmable piece marks malevolent applications simply implanted into necessary network. As we

know that controller does not have ability to discriminate applications on the basis of trustworthiness and validity by themselves. Far from that one ill efficient or fluted request could unauthorizingly bring new exposure sequence security defined networking. Hence for completing the trust of huge number applications this is really a big problem which should get solved early

**III. Possible Solutions to the Issues**

Some possible solutions to the issues are:-

• **Confidentiality and Integrity (C/I)**

Confidentiality and security of the system has important necessities which originate from network intrusion where for other network data and traditional network there is dissimilarity in innovative application. Attacker can pick control policies by overhearing data in terms of network about activities therefore data should be conveyed so that mischievous spying network crashing leakage and change should be avoided.

• **Authentication (Au)**

In network interaction, to promise the validity of an individual authentication significant benchmark. In security defined networking, many data interactions are present. Control plane's routing guidelines or application's new networks are even extra vital to the network. Without avoiding any authentication technique if these data are modified or provided by the attackers then the network will be tangled. According to the figures, authentication should be tarnished to confirm honest interactions among network bodies for associating the resistance on network intrusions in security defined networking and supervising the faith of network applications.

• **Fine-grained Access Control (FAC)**

In security defined networking model, good grained access control denotes subdivision of objects and each object provides specific access rights. In comparison to traditional controller access control is joined to other networking domain due to programmable service we need to provide every network programmer a good access privilege to guarantee application's appropriate function in first pass .Application trust management and network intrusion are associated to this constraint.

• **Self-healing (Sh)**

For reducing denial of service (dos) attacks and every kind of application or bug, self-healing is an important and noteworthy capability. The meaning of self -healing is that network devices can provide service and keeping itself in an anomalous state( by functioning it and also satisfactory level) possible errors, faults, trials and threats want to be recognized by consuming learning skills, for realizing self-healing in a prearranged communication network.

• **Revocability (Re)**

The dependability of an application must be assured. Application's privilege must be deprived if it performs maliciously. This necessity is supplementary to the application belief management.

• **Availability and Dependability (A/D)**

Availability and dependability confirms that a network permanently. For understanding this need security defined networking should be capable of boycotting any kind of DDoS attacks. In security defined networking design, availability\and dependability should be taken into justification.

## IV. FUTURE INITIATIVES

Security Defined Networking makes the operators as well as the respective Network owners to construct an easily maintained and controllable network .SDN would change the future of networking and will introduce fresh revolutions, according to a network research community. By keeping this thing in consideration, a good number of research creativities have been suggested the SDN prototypes and after that they were functioned on different campus networks, SD ratio and WN.

Different future research initiatives are:

• **SDN Prototypes**:

The main perception of SDN raised in the year 2005, But the writers presented 4d approach the management and network control. After this, fresh architecture ethane was defined which by centralized policies offered network control.

Ethane consumes centralized controller to control flow routing which embraces network policies. This too even utilizes Ethane switches that gain guidelines to forward packets to the respective endpoints from controller. Policies are programmed, if we use a flow centred security language created on data log. Ethane was installed in the Stanford computer science department ethane was installed to function 300 hosts as well as to assist 30 hosts in a small business. Ethane's distribution was a trial to estimate central network management it was a trial of ethane's distribution, which indicated that solitary controller, should maintain 10,000 original flow requests p/s for minor network schemes as well as scattered set of controllers could be organized for enormous network topologies. Using latest traditional network methods, Ethane is having two restrictions which preclude ethane from getting executed, At the beginning ethane, needs understanding regarding the network users in addition with nodes. Ethane claims regulation on routing on the flow level A network operating-system framework NOX, presented these drawbacks.

• **Virtualization as well as Cloud Computing in SDN**

For cloud-computing networks further current readings have established SDN-built controller framework, Meridian. Meridian makes available a network services. Model is made available by meridian that allows users to accomplish and create an appropriate commonsensical topology for the respective cloud capacities. In accumulation, virtual applications on fundamental physical networks are permitted by meridian. Stimulated by SDN, Meridian comprises three consistent layers: the network orchestration, network model in addition API layer also interfaces to network devices. Network modelmakes available the contact by means of network by declarative and query APIs. Declarative API produces a figure of multi-virtual machine use, whereas query API maintenances requirements for network statistics and topology views. The facilities for example arranging network alignment and control functions global view of data-center topology, routing algorithms are provided by orchestration layer. The interface to network devices which is the lowest layer is answerable on behalf of forming virtual networks. In accumulation to Meridian's significance in associate a service-level model, this is deliberated as preliminary SDN prototype in cloud. Researchers should be approximating to discover the Meridian's enactment in cases of complex workloads, this framework's scalability to backing enormous networks, and meridian's capability to pull through unsuccessful plans.

## V. SUMMARY

We know that security defined networking environment has continued its growth, the security of availability and privacy of every interconnected resource as well as information has become necessary. But it would be very difficult to gain security defined networking. There are conspiring statements regarding the perfect place where security defined networking should be kept perfectly.

Some people say that that security defined networking should be embedded inside the network whereas the other people assume that server, storage as well as other computing devices should have security with them.

Despite all these we could admit this that software defined network controllers need to be more and more secured as these are the centralized decision point in software defined networking. Attacks on security defined network controllers mean that we are compromising with SDN in its own environment. Controllers work as brain in SDN.

Change has made a new strategy for modern generation environment that is 'Software Defined Networking'. Software Defined Networking which is an example NFV (Network Function Virtualization) gives a new option to design display, deploy and maintain the various networking services. It does it by decoupling hardware application's network functions. For supporting virtualized infrastructure, important networking components are strengthened and are made for distribution. In software defined security, storage, server and other networks are included.

## VI. CONCLUSION

The main purpose of SDN is to make easier network architecture via centralization of the L3 routing equipment's control plane intelligence along with L2 switching. Security defined networking customs the foundation of network virtualization. Network hardware are advertised as a product service by SDN. SDN-compatible switches and the SDN controller are there in SDN architecture. The programmability as well as elasticity of SDN's architecture is manipulated by Academic researchers and network engineers so as to mark methodologies which make data-center LANs and WANs straight forwardly management and it even makes them more secured. For the reason that SDN makes it possible to make an agile as well as programmable network. Software defined networking supports NAAS (A latest Internet made model which behave as a connection in the middle of cloud computing and SDN).NAAS will distribute cloud tenant's packet-processing application, where as network administration and forwarding decisions are managed via SDN. In spite of entire auspicious occasions which go together with SDN, encounter assured technical experiments which power impede the functionality in the enterprises as well as cloud computing. For that reason, both IT organizations in addition with network enterprises have a duty to be attentive of these dares and discover SDN architecture's functionality to stand the respective disapprovals.

Though Security Defined Networking is an active, flexible and programmable as well as growing trendy approach, it's some of the major drawbacks could not be ignored. Every problem has solution .New ideas and alternates are needed to be generating so as to solve the security issues. Solutions need to be found out regarding the Security issues of Software Defined Networking so that we could easily get rid of these unwanted Challenges.

## REFERENCES

[1] http://www.comsnets.org/archive/2014/doc/ NickMcKeownsSlides.pdf

[2] http://opennetsummit.org/archives/oct11/shenker-tue.pdf

[3] https://www.youtube.com/watch?v=YHeyuD89n1Y

[4] OpenFlow. http://en.wikipedia.org/wiki/OpenFlow.

[5] Nick McKeown " OpenFlow: Enabling Innovation in Campus Networks", SIGCOMM Comput. Commun. Rev., pages 69–74, April 2008. http://doi.acm.org/10.1145/1355734.1355746

[6] Sandra Scott-Hayward, Sriram Natarajan and Sakir Sezer "A Survey of Security in Software Defined Networks". IEEE Communications Surveys and Tutorials, Vol. 18, No. 1, First Quarter 2016.

[7] Giotis, K. "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", Computer Networks, Vol. 62, Pages 122–136.

[8] S.Shin "AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks", Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS'13), pages 413-424.

[9] T.Xing Snort "Flow: A OpenFlow-Based Intrusion Prevention System in Cloud Environment", Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop (GREE'13), pages 89-92.

[10] Y.Wang "NetFuse: Short-circuiting traffic surges in the cloud", IEEE ICC-2013, pages 3514-3518.

[11] S. Lim "A SDN-oriented DDoS blocking scheme for botnet-based attacks" in Proc. 6th ICUFN, 2014, pp. 63–x68.

[12] R. Braga, E. Mota and A. Passito " Lightweight DDoS flooding attack detection using NOX/OpenFlow", in Proc. IEEE 35th Conf. LCN, 2010, pp. 408–415.

[13] Sungmin Hong "Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures" NDSS'15.

[14] Bob Lantz, Brandon Heller and Nick Mckeown, Hotnets-IX, " A network in a laptop: rapid prototyping for software-defined networks", Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Article No. 19, 2010.

[15] Mohan Dhawan " SPHINX: Detecting Security Attacks in Software-Defined Networks", NDSS'15.