International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

A Survey on Security in Software-Defined-Networking

Tapan Rai, Nikhil Bansal, V. Deeban Chakravarthy

Abstract—With the development of data and systems administration advancements, ordinary system frameworks have not had the capacity to adapt up to the expanding request. To meet this requirement SDN (Software Defined Networks) was proposed; the idea was simply to decouple the control layer, the application layer and the infrastructure layer and connect them using application programming interfaces or APIs. SDN empowered network managers and gave rise to automated network management which is evident in the cloud infrastructure of today. Notwithstanding, there are many system security issues with respect to SDN, which require problem solving. In this paper, we undertake a survey for the field of security implementations in SDN and review existing countermeasures against known threat to the network.

Index Terms - Software Defined Networking, OpenFlow, Network Security, Denial of Service

I. INTRODUCTION

With the development of data and systems administration innovations, traditional system frameworks have not had the capacity to adapt up to the requests of viable applications and system clients. In this period of globalization and data blast, networks are expected to be highly efficient, stable, flexible and agile, they need to work where traditional network routing methodologies fail. Meanwhile, traditional networks are hard to upgrade as they require manual upgradation using vendor-specific commands. Software Defined Networking (SDN) makes it conceivable to get through the confinements of current system mode by physically isolating the forwarding usefulness known as the data plane, from the logically centralized control place where the management of entire network relies. This system overlooks the distinctions in the gadget foundation, and gives the administrators an easier method to deal with the system through Application Programming Interfaces (APIs). SDN was conceived at Stanford University in 2006 and increased critical footing in the business with quick advancement in these years. This prompted the making of the ONF (Open Network Foundation), a client drove association devoted to advancement and appropriation of programming characterized systems administration.

The ONF was responsible for the creation of OpenFlow [1], the principal standard correspondence interface characterized between the control and forwarding layers of a SDN design. The popularity of OpenFlow in the field of academic research and industry wide adoption further led to the development of SDN. With such fast paced growth security is obviously an issue of extreme importance, due to SDN's application of unified control and complicated flow tables, it has become a focus for harmful users to exploit the network. The goal of this paper is to assess and summarize security threats in SDN in order to identify future research directions on the basis of properties of any secure communications network that are classification, integrity, accessibility of data, validation and non-revocation[2].

II. SDNARCHITECTURE

SDN essentially decouples the existing control plane and forwarding plane functions and separates them into individual entities. The control place remains as a set of protocols and programs which guide the real world implementations in the forwarding plane, this provides a layer of abstraction between the network devices and applications.
In SDN, the controller is responsible for controlling the forwarding plane consisting of network devices in real-time using programmable instructions. This allows network operators to be able to change business requirements and redefine their network architecture as and when required. The SDN architecture is represented in Fig. 1. As shown in Fig. 1, a network operator can actively change the network interface routing and security policies using the controller. The three layers of SDN under the OpenFlow Architecture are as follows.

1. Application Plane: The application plane consists of programs that are programmatically responsible for manipulating the network by communicating the desired network requirements using the Northbound API. They are responsible for providing the user with an abstracted view of the network and acquiring and managing the state of the network and all its components. Fig.1 depicts the application plane as the top level in the SDN architecture consisting of security applications, operator services, management applications, monitoring applications and vendor applications.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Tapan Rai*, Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.
Nikhil Bansal, Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.
V. Deeban chakravarthy, Asst. Professor(Sr.G), Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.

It is the hub for all network changes and operations related to the network. The application plane is also the most insecure layer in the whole architecture as its under constant human interaction and is basically a password protected admin panel for controlling the entire network for an organization.

2. Control Plane: The controller is the central plane in the SDN architecture that is responsible for translating the networking requirements of the application plane and manipulating the network to reach the desired state. It resides on the receiving end of the Northbound API and is responsible for receiving and implementing the instructions forwarded by the Application. The control plane works with application specific APIs to decode and understand instruction from the application plane using the NBI. The control plane is a highly scalable layer as it contains simple machines processing and passing instructions from the application pane to the data plane. It is relatively secure compared to the application plane as the only point of contact is the application which can be cut off if and when a breach is detected.

3. Data Plane: The data plane is the actual hardware layer which consists of network devices such as routers, access points, switches, hubs etc. which are actually responsible fro routing all communication and keep services working. The data plane is the lowest level of the SDN architecture and these devices are controlled and configured by the upper levels. They are managed using instructions from the control plane via RPCs (Remote Procedure Calls).

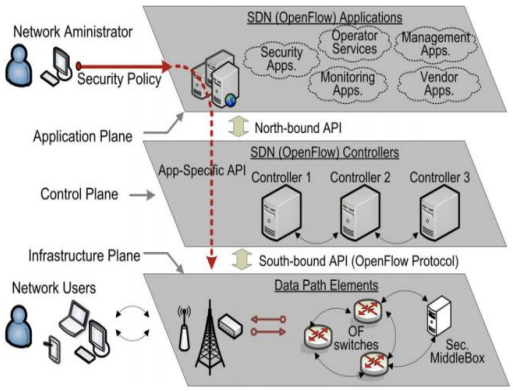

Fig. 1. SDN Architecture

SDN utilizes the forwarding plane by simply using the infrastructure as interconnecting devices which function by forwarding packets using routing policies of control plane. The control plane act as the brain of the entire network, its prime task is to collect the running status of underlying devices and is used by network operators to formulate routing policies and instructing the actions of forwarding plane devices. Generally, SDN controllers operate in clusters managed by a master controller. In complex network architectures we observe cluster intersections where several controllers would belong to independent or non-independent clusters and the application plane would be responsible to monitor and configure network functions. The application plane is responsible for generating network policies and network applications like load balancers, intrusion detection system etc.

The two most common characteristics of SDN are the centralization of network control and the programmable interface for network creation and control [3]. These features make the functionality revision and network management extremely simplified in comparison to the operation of traditional networks. However, because of these features, it becomes a prime target for internal attackers and users. The centralized nature of SDN makes it vulnerable to Denial of Service (DoS) attacks. So anyone who has access to the application plane's host or the controller can very easily get hold of the control of the entire network. A number of these threats have been presented in [4]. According to the second characteristic, any person with knowledge to programming can manipulate the network, this make it hard to distinguish between legitimate and harmful applications. This makes application trust management a very important issue to attend to.

III. EXISTING SYSTEM

In [5] it is stated that SDN does have a security benefits compared to normal network deployments but there are very few solutions in the field. WIth the rise of cloud computing environments and attacks happening on a larger scale, it has become very difficult to detect and mitigate. Till date there are not foolproof methods to prevent DDoS attacks.

Let us talk about security issues with programming characterized systems administration so as to condense its security necessities. Now let us look at three major SDN security issues: arrange interruption, forswearing of administration, and application trust the board. Not quite the same as the conventional networks, the issues discussed here require new security protocols to be implemented on SDN networks.

1. Network Intrusion: A Network Intrusion is an unapproved access on a computer network. System interruption is a major issue in the conventional networks. The value of using SDN to provide intrusion detection is proposed in [6] but due to the centralized nature of control plane implementation an attack like network intrusion is even more harmful as the attacker can get access to the whole network. As of now no effective methods have been developed to properly prevent intrusion into the network. Safeguard methodologies aimed to this security issue incorporate firewall, access control, intrusion detection and so on.
2. Denial of Service: One of the greatest security shortcomings in SDN is DoS/DDoS assaults. Because of the logically centralized nature of SDN it is extremely susceptible to denial of service attacks, namely, TCP-SYN flood, HTTP flood and ICMP flood [7]. A packet flood of extensive payload will render the storing system in switches useless and the controllers will debilitate its processing power to manage the huge amount of useless queries causing the entire system to crash.

3. Trust Management: Trust, and Trust Management assumes an imperative job in the use, unwavering quality of administrations, and framework also [8]. The programmable component makes it simple for vindictive applications to be implanted into the system. SDN applications lack the trust management system to distinguish between malicious, trusted applications and poorly designed or buggy applications.

IV. CHALLENGES IN SECURITY

The separation of the control plane into a centralized system opens the current network to new security challenges. The divided architecture becomes more susceptible to attacks like Denial of Service and Distributed Denial of Service attacks. The controller can become a single point of failure for the entire network during a security compromise. In this sections we discuss security challenges with the SDN architecture concentrated around all three planes of application, control, and data. The issues are described below.

1. Application Plane: The application plane consists of interaction most operators have with the network and developing an application opens the network to numerous security risks. These risks are elaborated on below.

a. Authentication: Implementation of proper authentication systems in the current fast paced software development scenario is a major issue while developing SDN applications. Due to lack of technologies to create proper trust relationships between the controller and application planes any malicious application can cause potential havoc to the whole system.

b. Access Control: Proper implementation of ACL is required is any digital application to preserve the CIA triangle of confidentiality, integrity and availability in database security. Since most application used today are based on SDN, a compromised network can become a gateway to the application itself.

2. Control Plane: The control plane has an important role to play for the SDN architecture to work which makes it a serious target for attackers to compromise the network. The security challenges faced by the control plane are as follows.

a. DoS Threats: DoS is the most dire security threat for an SDN controller. DoS is a network attack where the attacker attempts to make the attacked resource unavailable to use by flooding it with malicious data packets which puts the resource in a non-responsive state.

b. Compromised Application Plane: The Application plane operating on top of the control plane poses serious security risks. Improper authentication and authorization implemented on the application side can provide attackers with some if not all functionality of the control plane which will be disastrous for the network.

3. Data Plane: The higher levels in the SDN architecture are responsible to control the data plane and networks associated with it. All invalid and potentially disastrous configurations can also be passed to the data plane if security is compromised.

The defense instruments against system/transport-level DDoS flooding assaults can be grouped into four classes dependent on the deployment location :

1. Origin-based mechanisms: Origin-based systems are conveyed close to the wellsprings of the assault to keep arrange clients from producing DDoS flooding assaults. A few instances of source-based instruments incorporate entrance/departure sifting, which channels bundles with satirize the IPs at the origin's edge routers dependent on the substantial IP address extend inward to the system, and the SAVE Protocol. Spare convention engages changes to revive the information of expected source IP addresses on every association and square any IP package with an unanticipated source IP address.
2. Network mechanisms: These mechanisms are launched on the routers inside the networks to prevent attacks. There are basically two types of DDoS attacks recognition techniques namely ASD (attack specific detection) and ABD (anomaly based detection). SYN Flood involves flooding a target computer with spoofed SYN packets containing fake source addresses. Flooding overwhelms the victim's computer and depletes it of its resources causing performance degradation and overall shutdown of the system [10]. On the other hand an ABD system analyzes the behavior of usual network packets, and then reports any anomalies in them.
3. Destination-based mechanisms: Defense methods that come into action at the destination of the attack are known as destination based defense mechanisms. Probabilistic packet marking, Input debugging , hash-based IP traceback are only some of the destination based prevention mechanisms. Input debugging uses iterative testing of upstream links to discern attacking traffic, it is a link testing mechanism. In probabilistic packet marking, routers are marked based on probability calculation of them being in the path to the attacker traffic origin which helps in retracing the attack to the attacker and distinguish it from legitimate packets. This sometimes upsets the packet division methodology, nevertheless the frequency of fragmentation is arguably below typical packet loss rates [10]. In the hash-based IP traceback method, routers are responsible for keeping a hash record of every packet going through their system using a bloom filter.
4. Distributed mechanisms: Distributed defense mechanisms are deployed at different areas, like, at the origin, goal or middle of the road systems and there is generally cooperation among the arrangement focuses (for example AITF (Active Internet Traffic Filtering)), which empowers

a collector for contacting acting up origins and request that they quit sending its traffic). In AITF, each switch contract controls the traffic traveling through it to allow policing the requesting and adequately filtering them through [12].

We outline security prerequisites of SDN so as to beat the above security issues. These prerequisites are criteria to ensure the system, which are likewise used to assess the nature of SDN security arrangements.

1. Classification and Integrity (C/I): They are the key prerequisites to verify any framework. Information must be transmitted safely over transport layer encryption to keep from malevolent listening in, changing, spillage and system crash as an aggressor can derive control strategies by spying the information about system activities.
2. Authentication (Auth): Authentication is an imperative rule to ensure the authenticity of a personality in a system communication.There are numerous information interactions in SDN. Without proper authentication methodology, data regarding routing instructions and network functionalities can be delivered by attackers and render the network unusable. Authentication works to ensure trustworthiness in network operators.
3. Access Control (AC): Access Control refers to dividing control layer operations access into user specific roles and assign operators the said roles. This gives each system programmable a fine grained access to guarantee legitimate working of the system and in the meantime keep any unapproved changes.

V. RESULT

From the above explanations some implementation techniques can be extradited which are responsible for leaving software defined networks exposed and vulnerable to different kinds of attacks. In these, the most dangerous is the centralized implementation of controllers which makes it a single point of failure for the whole network. Followed by centralization, improper implementation of security protocols is another big factor leading to vulnerable networks.

VI. DISCUSSION

It can be derived from the current scenario that software defined networks are an inevitable part of current technology standpoint as it is the backbone for all cloud applications. The rate at which cloud native implementations are growing in number it becomes exponentially important for our networks to be secure and highly available as the number of users on these applications increase.

VII. FUTURE EXPLORATION DIRECTION

Issues like this persuade us for further research work. To begin with, so as to conquer the assaults raised by harmful applications, a trust management system for SDN needs to be investigated. Step by step instructions to assess management of the applications in the SDN application plane dependent on their execution and impacts on systems administration security is as yet an open issue. Instructions to set up an incorporated and tenable trust the executives framework that can be utilized to deal with a mass of uses in SDN is a fascinating examination heading. Next, we referenced the criticality of the channel for security correspondence among the application and the control plane. Additionally, a uniform SDN security configuration is required. The present work simply revolved around fragmentary security issues in SDN. Nevertheless, paying little respect to the conflicts between different strategies for securing SDN, and dealing with these disputes in functionality and to unite them in a safe and secure manner is difficult. Finally, a lot of DoS area and moderate procedures basically stay on a theoretical measurement or simply be attempted under a little scale arrange topology. This is far to meet the security necessities of a veritable framework condition. The future research should give a fantastic thought to execution of these game plans in order to survey them in a by and large reasonable and authentic condition to guarantee they can work effectively

VIII. CONCLUSION

As another innovation, SDN has turned into an intriguing issue in the IT business. The ramification of forwarding and control planes influences this new plan to have extraordinary points of interest for supporting system adaptability and management. But the ubiquity of SDN needs to ensure its security and validity. In this paper, we displayed a broad overview of issues and countermeasures on SDN security. We broke down three sorts of security dangers and outlined the current works identified with them. With the exception of this, we utilized the security prerequisites to assess the current work. In view of the talk on open issues found through our overview, we proposed some significant future research bearings of SDN security.

REFERENCES

1. N. McKeown et al., "OpenFlow: Enabling innovation in campus networks", ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, 2008.
2. C. Douligeris and D. N. Serpanos, “Network security: current status and future directions”, 2007.
3. B. Raghavan et al., "Software-defined internet architecture: decoupling architecture from infrastructure", Proc. 11th ACM Workshop Hot Topics Netw., 2012.
4. S. Sezer, S. Scott-Hayward, P. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," Communications Magazine, IEEE, vol. 51, no. 7, 2013.
5. S. Scott-Hayward, G. O'Callaghan, S. Sezer, "SDN security: A survey", Proc. IEEE SDN4FNS, 2013.
6. S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in Recent Advances in Intrusion Detection. Springer, 2011.

7. Ko C, Ruschitzka M, Levitt K, “Execution monitoring of securitycritical programs in a distributed system: a specification-based approach [C]/Proc of IEEE Symposium on Security and Privacy”. Washington DC: IEEE Computer Society, 1997.
8. M. Firdhous, O. Ghazali, S. Hassan, "Trust management in cloud computing: A critical review", CoRR, 2012.
9. Yan, Qiao, Richard Yu, Qingxiang Gong, and Jianqiang Li. "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, 2015.
10. K. Geetha ; N. Sreenath, “SYN flooding attack — Identification and analysis”, ICICES2014, 2014.
11. D. Dean, M. Franklin, A. Stubblefield, "An algebraic approach to IP traceback", Proc. Network and Distributed System Security Symp. (NDSS), 2001.
12. Katerina Argyraki, David R. Cheriton, “Active Internet Traffic Filtering: Real-time Response to Denial-of-Service Attacks”, 2003.

AUTHORS PROFILE

Tapan Rai, UG Student Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.

Nikhil Bansal, UG Student Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.

V. Deeban chakravarthy, Asst. Professor(Sr.G), Department of Computer Science Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Tamil Nadu.