ORIGINAL RESEARCH PAPER

Engineering

Volume - 7 | Issue - 2 | February - 2017 | ISSN - 2249-555X | IF : 3.919 | IC Value : 79.96

# SDN Security Issue and Resolution

KEYWORDS

Software-Defined Networking, Virtualized Environments, Network Function Virtualization.

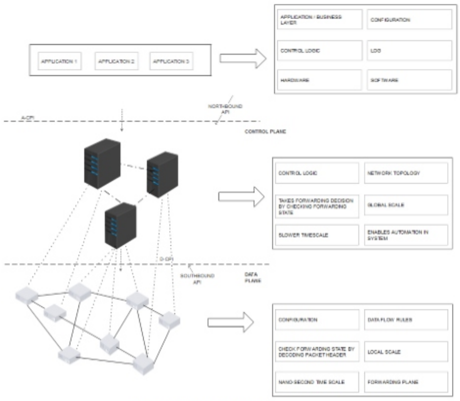
| Himanshu Kumar | Prabhav Gupta |
|---|---|
| Btech(CSE) Student, SRM University | Btech(CSE) Student, SRM University |

ABSTRACT *Computer Networking has established itself as one of the convenient way of resource sharing such that today businesses and organizations heavily rely on it to send information across communication points. However, the current adaption of networks is hard to evolve, manage and network design has not much to offer. In order to overcome the problems with traditional networking techniques, Software Defined Networking (SDN) was introduced as an emerging architecture that supports modern networking requirements and has a programmable approach to the network control. Since this way of networking has the potential to be widely adopted in the coming times, it becomes a point of interest for attackers to exploit vulnerabilities to gain access to system assets. The objective of the article is to analyse significant vulnerabilities to SDN architecture and propose suitable security solutions for the model that can tackle the most, if not all security concerns through some pre-existing attack vectors, which poses a possible threat for the existing model. This article intends to guide on importance of virtualized environments and running of SDN along with Network Function Virtualization(NFV) infrastructure. In summary, new era in building networks and providing suitable security is upon us.*

## 1. INTRODUCTION

Today networks are far more complex than just static architecture of traditional networks and when compared to dynamic computing or ever increasing network demands [1], the dimensions to computing and data traffic remain very much restricted. The transfer of data is a much complicated process involving different areas of operations which majorly involves three integral layers namely data plane, control plane and application plane. The data plane carries the user traffic, control plane decides through various routing protocols which path does the information through data plane travels. Thus data plane checks the forwarding state by decoding the packet header and control plane computes the forwarding decision by checking the forwarding state. Various business and commercial applications designed today to simplify the needs of the consumer run on the Application Layer. In nascent technology adoption these planes are implemented in firmware of physical devices which means packet forwarding and high-level routing take place on the same device. Due to which traditional networking architectures have reached till a point where it's ability to adapt dynamic environments have become hindrance. This becomes the reason that coming up with a secure solution has grabbed the focus of great deal of attention both in terms of academic research and application in real world.

Whereas SDN works on the basic principle [2] of decoupling the data plane from control plane thus, creating a management system which effectively takes away all the intelligence from the networking equipments and a separate physical device, a controller, holds all of the central intelligence of the system. Considering dynamic nature of today's applications, SDN seems to be the best solution for coping up with drawbacks of traditional networking techniques as discussed in [3].



ARCHITECTURE AND OPERTAIONS OF VARIOUS PLANES

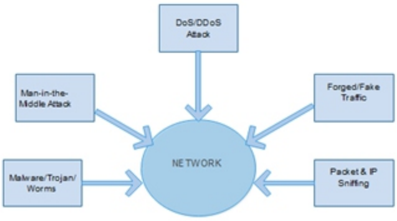
SDN aims towards creation of high level network policies by development of open API's, such that applications could be network aware not application ambivalent. SDN introduces new risks and challenges but the advantages considerably outweigh the negatives which are various security breaches and loopholes that can be mitigated by providing suitable solution.

## 2. BACKGROUND

As SDN is an emerging networking architecture, it grabs the attention of hackers and varieties of attacks continue to increase. Securing the system becomes the dire need in order to protect privacy of all connected physical devices in the network alongside the confidential user information. But securing SDN can turn out to be a tough job. Since, attacks on SDN Controllers means compromising the whole network itself. OpenFlow [4] is the most noticeable and appreciable implementation for SDN deployment. So, it becomes primarily essential to identify the major interest in mitigating security problems of OPENFLOW PROTOCOLS. This analysis helps in projecting the schemes for breakthrough of various emerging protocols. Since SDN and OpenFlow both have different dimensions of security threats and aspects added to them. Vulnerabilities present in OpenFlow such as network congestion exploitation and inadequacy in monitoring functions are a result of its rapidly evolving nature. Network congestion [5] occurs when a network node is carrying more data than it can handle, there is the potential for a bottleneck when devices send control messages to the controller. The communication path to the controller, and possibly the controller itself, is overloaded, leading to the removal of some messages which corresponds to data loss. So, an attacker could attempt to exploit this vulnerability by sending a large number of packets to the network which do not correspond to existing flow rules. Thus in this state the controller can't establish to make routing decisions, so if these issues tend to appear continuously then it's possible to flood data plane with syn packets [6] and successfully establishing a DOS attack. Secondly, while monitoring control layer functions request for statistics and the response from switches must traverse the control communication link. These requests regarding statistics must be requested by the controller. But there is no specific method designed for grouping them to reduce link usage. Thus, now events in the data plane like deciding the forwarding state of the packet are now delayed. Some of the major vulnerabilities exist within the SDN architecture. As SDN systems are equipped to take defense actions automatically [7] whenever it is exposed to some threat, but as attackers keep coming up with new methods to steal crucial data they tend to perform attacks that look legitimate to the network creating confusions or they can easily trick system to believe that it is under attack. Now system will deploy its defense mechanism which can cause delay to make forwarding decisions for data plane since these countermeasures require lot of resources to launch themselves. However, developing these defense mechanisms inside the system is not enough for analysing the critical conditions of SDN controller. Thus, advanced security measures need to be taken for securing the whole architecture. By performing a simple man in the middle attack [8], attacker can tamper the on-path traffic which alters network behaviour. Attacker alters the communication between host and client who still falsely believe that only they are the two parties engaged. But attacker can now jack identities, steal credentials. At this level the least that can be done is to encrypt data packets but even it fails to protect control data from being leaked.

## 3. ATTACK VECTORS

Attack Vectors are the surfaces prone to threats in the system architecture [9] through which attackers can exploit system loopholes.



THREATS COMMON TO TRADITIONAL AND SDN NETWORKS.

a) Trust between controllers and applications: Most of the times the SDN controllers run on some form of Linux based OS. These controllers do not establish rules of trust for applications and don't have mechanisms in order to establish trust. The attackers will desperately try to bog the controller [10] causing it to respond extremely slow, such that there is considerable amount of time delay for transferring data. Also, the attacker can generate new flows by spoofing northbound API message toward application or spoofing southbound messages toward the network devices giving him ability to control the traffic that flows and possibly exploiting the policies that maybe relied upon for security [11].

b) Physical devices: Malware infection at runtime results in Switch Device Firmware Abuse meaning physical device has been compromised which can be revealing enough [12] for exploiting other resources in the network and leaking information out. Such attacks can lead to unnecessary deployment of countermeasures consuming resources and exploiting other weaknesses in the network.

c) Authentication, Authorization &Accounting: AAA are three distinct components that are essential primitives for SDN which help in the process of identifying a user, determining the permissions granted to that user and keeping a record of the accessed resources. Thus, users can now uniquely be identified by assigning these attributes and system can use that information to identify access control policies [13] to determine what privileges are granted to the operator who has been authenticated. These three essential primitives are the basis for forming a securing a secure network which helps us to identify vulnerable or bad nodes and isolate them from the open or listening ports. But Lack of or inefficient response system during the authentication through remote clients could cause attack on the management interfaces, so if now an attacker gets in the system he can manipulate logical network topology maintained by SDN controller to cause fatal network failures.

d) Controller vulnerabilities: The controllers have a number of weaknesses, weaknesses that can far exceed the protocol. Floodlight is a java-based open-flow controller whose northbound HTTP API has no encryption and no authentication. Also Open-daylight which is largest open source SDN controller does have encryption on the northbound HTTP API [14] but it is turned off by default. It has authentication but it is HTTP Basic Authentication, the default password is weak, and strong passwords are turned off by default. So even a simple brute-force attack can be quite revealing in nature about topology of the network as well as credentials.

## 4. SDN-SECURITY SOLUTIONS

The security and integrity of software-defined networking remains unproven, particularly the controller, which is a single point of failure. So in order to address this problem we can adapt to the use of elastic distributed controller architecture also known as elastic-on [15] that operates by logically centralising the control plane which is physically distributed and addresses the issues like scalability and reliability of SDN networks in a much more improved and certainly more improvised way. Due to the load imbalances which occur due to aggregate load changes, the networking flow starts to show random trends so it makes much more sense, to migrate a switch from heavily loaded controller to a lightly loaded one. Thus this expanding or shrinking of controllers from the spatial pool solves our problem of direct attack on the controller in control plane. Though this does not mean that attacker now cannot attack the control plane but definitely improves by providing more security than the existing architecture.

Cyber attackers employ sophisticated deception techniques designed to disrupt the functioning of the control plane by IP specific attacks. Thus in order to deceive the attackers, we can adapt to MTD (Move Target Defense) paradigm which is implemented using virtualization and workload migration. Network level MTD [16] includes vast variety of mechanisms for example, IP-hopping, is used to change the host's IP address thus making the network more complex for attacker to analyse. Real host's IP address can be associated with some virtual IP address, and because it is going to be completely random it makes attacker operate in a completely uncertain environment. Some techniques associated with MTD possess capability to deceive the attacker at phase of reconnaissance. These techniques majorly aim at providing attacker with fake system dimensions like host and OS type or version which is achieved by usage of fake listening ports which means either extra open or closed ports, randomly choosing ports etc.

Encryption is one of the ways of protecting the data from being exposed. But even together with the integrity protection which acts as a centrepiece of protection for system owned files and directories against modification by a specific "entitlement", executed by the root user or any user with root privileges. The combination of encryption and integrity protection [17]is not sufficient to protect the network against man-in-the-middle-type attacks. So, the security can be enhanced by using mutual authentication. Mutual authentication advances protective threat measures, provides integral protection and preserves users confidentiality. Though mutual authentication does have a difficulty in bootstrapping security into the system. In order to further increase systems security, required certificates must be issued and installed or revoked accordingly under systems administrator knowledge at regular intervals. Thus network now becomes much more difficult to penetrate.

## 5. SDN DEPLOYMENT

The prominent problem with traditional networking techniques is that it fails to address the issue of network agility, such that network software and hardware cannot control and configure themselves according to the desired needs, so they always need manual supervision thus ending the whole process of setting data centres laborious. SDN provides automation (intelligent decision making) to encounter problems that have to be made in real time such that system can now pro-actively respond to the real time conditions according to the configuration of the network.

The automation in the system can be achieved by using customised tools according to the requirements of administrator. With the progressing researches, an evolution was made to virtualize [18] the network services that were till now being carried out on a dedicated hardware. This technique of Network Function Virtualization (NFV) suggested once the network functions (Firewalls, IPS, Load Balancers etc.) are being controlled by network hypervisor the services that required dedicated servers can now be hosted on standard x86 servers. Hence guiding principle behind NFV remains is the separation of control functions and forwarding functions. These approaches of networking architecture are beneficial in their own ways [19], but don't always need to operate together and whatsoever don't depend on one another for their functionality.

SDN is a concept practised by large-scale vendors as well as seems to be quiet promising for small business setups, where networking engineers intend to simplify traffic management and achieve operational efficiencies by establishing and exercising central control over policy-based decisions which manage data flow to orchestrate network traffic while NFV focuses on various business critical services, and ensures virtualized environments are capable enough for the smooth working of network functions over the network. Now when SDN runs on NFV infrastructure the issue of network agility appears to be much less complex. Hence this type of deployment has an endless future potential.

## 6. CONCLUSION

The proposed work was aimed to present an explicit detail of a secure SDN model. A deployment has been structured but threats continue to prevail in the system and securing it becomes the prime concern and this workflow is based on evaluating threats and developing mitigation strategies based on these threat vectors. Organisations should conduct threat modelling which helps to identify all the threats possible to SDN deployment model at an early design stage. By gathering the previously existing analysis [20] [21] of security flaws found in other SDN systems and gaining knowledge about the trends of the attacks that continue to prevail, can help to predict future attacks and develop various secure test models to protect the architecture.

Along with the continued technical security measures such as trust systems, integrity checking and recovery mechanisms. The salient features of the research article include:
1. Security by elastic distributed controller architecture,
2. Adapting network level MTD and
3. Developing a strong encryption mechanism.

Till the time we come up with inclusive security architecture in SDN and overcome the drawbacks proposed in SDN models, solutions are going to be only partially effective. Therefore, it becomes equally important to put focus on defense mechanisms as well as trust systems. In a nutshell, the implementation of these technologies [22] either or both SDN & NFV will be dependent on future needs of this market which has a never ending potential for expansion. Though yet SDN, needs some time to mature so that major vendors can adapt to this technology at a rapid pace. Hence it is true to say that future networks will revolve around SDN based networking.

## 7. REFERENCES

1. Wenfeng Xia, Yonggang Wen, Chuan Heng Foh, Dusit Niyato, and Haiyong Xie, "A Survey on Software-Defined Networking". IEEE Communication Surveys & Tutorials, Vol.17, No.1, First Quarter 2015.
2. Masayoshi Kobayashi, Srini Seetharaman, Guru Parulkar, Guido Appenzellerq, Joseph Little, Johan van Reijendam, Paul Weissmann, Nick McKeown NEC Corporation, Deutsche Telekom, Stanford University, Big Switch Networks "Maturing of OpenFlow and Software Defined Networking through Deployments" Pg. 1-4.
3. IP KNOWLEDGE http://www.ipknowledge.net/wp-content/uploads/2014/12/SDN.pdf
4. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson Jennifer Rexford, Scott Shenker and Jonathan Turner, "OpenFlow: Enabling Innovation in Campus Networks" March 14, 2008.
5. Sandvine Intelligent Broadband Networks, "Network Congestion Management: Considerations and Techniques. An Industry Whitepaper (Version 2.0).
6. Karthik Lakshminarayanan, Daniel Adkins, Adrian Perrig and Ion Stoica, "Taming IP Packet Flooding Attacks". ACM SIGCOMM Computer Communication Review Volume 34 Issue 1, January 2004.
7. Haifeng Zhou, Chunming Wu, Ming Jiang, Boyang Zhou, Wen Gao, Tingting Pan and Min Huang, "Evolving defense mechanism for future network security. IEEE Communications Magazine (Volume: 53, Issue: 4, April 2015).
8. Mauro Conti, Nicola Dragoni and Viktor Lesyk, "A survey of Man in the Middle Attacks". IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 3, 2016).
9. Christian A. Christiansen Michael Versace "Securing the Datacentre from Advanced Threats". Sponsored by: Juniper Networks Inc. Page 5-6
10. K. Cabaj, J. Wytr bowicz, S. Kukli ski, P. Radziszewski and K. Truong Dinh,"SDN Architecture Impact on Network Security". Position papers of the 2014 Federated Conference on Computer Science and Information Systems DOI: 10.15439/2014F473 ACSIS, Vol. 3.
11. Kristian Slavov, Makan Pourzandi and Daniel Migault, "Identifying and addressing the vulnerabilities and security issue of SDN". CHARTING THE FUTURE OF INNOVATION Vol. 92 | #7.2015.
12. Seungwon Shin, Lei Xu, Sungmin Hong and Guofei Gu, "Enhancing Network Security through Software Defined Networking (SDN)". SUCCESS Lab, Texas A&M University.
13. http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-35/101-aaa-part1.html.
14. Seungwon Shin, "Software Defined Networking Security: Security for SDN and Security with SDN". Network and System Security Lab, GSIS, KAIST.
15. Advait Dixit, Fang Hao, Sarit Mukherjee, T.V. Lakshman, and Ramana Kompella, "Towards an Elastic Distributed SDN Controller". Bell Labs Alcatel-Lucent
16. Rui Zhuang, Scott A. DeLoach, Xinming Ou, "Towards a Theory of Moving Target Defense". Kansas State University Manhattan, KS USA
17. Changhoon Yoon and Seungsoo Lee, "Attacking SDN Infrastructure: Are we ready for the next-gen networking?". Black Hat USA 2106
18. "Service-aware network architecture based on SDN, NFV and Network Intelligence", WHITE PAPER Intel Architecture Processors Qosmos * DPI Technology.
19. SDN 101 and more IE stuff Chapter 28 Virtualization Pg.100-103 https://www.docdroid.net/IadFYf6/sdn-101-and-more-ie-stuff.pdf.html
20. Anthony Lim, "Security Risks in SDN and Other New Software Issues" in RSA Conference 2015 at Singapore (Marina Bay Sands).
21. Sandra Scott-Hayward, Sriram Natarajan, and SakirSeze, "A Survey of Security in Software Defined Networks" in IEEE Communications Surveys and Tutorials 18(1), 623-654. DOI: 10.1109/COMST.2015.2453114
22. Deloitte, "Operationalizing SDN and NFV Networks". May 2015 Deloitte Consulting LLP.