ACTA SCIENTIFIC COMPUTER SCIENCES

Volume 1 Issue 2 December 2019

Research Article

Security and Scalability in Software-Defined Networks

Cheryl Ann Alexander[1]* and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Vicksburg, USA*

***Corresponding Author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA.

Received: November 18, 2019; **Published:** November 29, 2019

Abstract

Software-defined networks (SDN) are becoming more popular today as researchers seek to find novel solutions to the challenges present in our Internet, social media usage, and the numerous threats to data. One of the most promising technologies today is the SDN as we need a higher level of security, stronger equipment, and more data privacy. In this review paper, we discuss and explore the state of SDN, the benefits and disadvantages to this upcoming technology, challenges and future work.

Keywords: Software-Defined Networks; Scalability; Open Flow; Network Virtualization; Cloud Computing

Abbreviations

Software-Defined Networks (SDN), Internet of Things (IoT), Distributed Denial of Service (DDoS) attack, Network Service Providers (NSP), Host-Based Intrusion Detection System (HIDS), Open-Source Host-Based Intrusion Detection Security (OSSEC), Network Function Virtualization (NFV), Moving Target Defense (MTD), Random Host Mutation (RHM), Internet Protocol (IP), Moving Target Defense (MTD), Fuzzy Self-Organizing Maps-Based Mitigation (FSOMDM).

Introduction

Today, cyberspace has become a critical part of the core of social structure. With the enrichment and extension of networks, services, and applications, underlying devices such as switches and routers have become key to networks. Control network architecture forward separation, which is a networking development trend, needs high-level security and high-quality service of the network is also necessary. One of the most promising network technologies is Software Defined Networking (SDN) [1]. In SDN, high-level tactics are defined by the exclusive equipment which is used to channel the data forwarding of the network equipment. This results in a reduction of the many complex functions of the network equipment and improves the plasticity and operability of the implementation and deployment of new network protocols and technologies. However, this novel networking technology faces challenges in terms of architecture, scalability, and security [1]. In addition, SDN, has brought new features and offers more elasticity than the average network results. SDN fosters effortlessly managed controllability based on standards-based software constructs of the network infrastructure. This is easily achieved by detaching the control plane (i.e., control logic) from the logic plane (i.e., forwarding plane). Based on this network model, the routers and switches are limited to forwarding traffic only. The control logic is then central within a controller which characterizes the network operating system of an SDN network and plays a significant role in managing flow control and configuring network elements of the data plane using such protocols as OpenFlow [2].

Numerous novel networking concepts to simplify network management and create innovation through network programmability in the cloud. SDN also guarantees easy management as it eliminates the network infrastructure maintenance processes. By responding in this manner, SDN can offer real-time performance and responses to high availability requirements. However, there are certain challenges facing SDN currently, primarily scalability and security.

Some of the challenges facing SDN are inherent, however, some facing this technology are brought about by adopted technologies themselves [3]. An innovative approach to network management, SDN separates the control plane from the data plane making network management much easier. By separating the data plane from the control plane, SDN has more flexibility, controllability, and a better user experience. This segmentation delivers many benefits in terms of controllability and flexibility. It also creates a fine line between combining the advantages of network virtualization and cloud computing. This implements a centralized intelligence, which enables making a clear visibility over the network to create an easy network while at the same time an enhanced network and control. However, in a traditional infrastructure network, implementation, troubleshooting, and configuration require a higher level of engineering control and intervention, also operational costs associated with provisioning and managing large networks. Therefore, scalability and security become an instant issue and trying to connect with a business network also puts the network at risk [3].

The future of network innovation is SDN. This pioneering technology has revolutionized the networking world for a decade and continues to renovate legacy network architectures. However, security for SDN remains too casual and researchers do not seem to take it seriously enough. Detailed attacks on SDN networks and techniques to deal with them will be discussed further. Some considerably defenseless attack areas in SDN which can lead to severe network attacks will be considered. These attacks could be assaults on the controller, attacks on network devices, attacks exploiting the communication link between the control plane and data plane, and various types of poisoning on topology. It is necessary to propose some methods to handle the SDN attacks [4].

The importance of software-defined network security

Both industry and academia have increased their interest in SDN lately because it is more efficient at decoupling the control panel from the closed predesigned networks, therefore, SDN fosters the capability of network devices such as IoT, sensors, etc. In the past, traditional network devices could only work as they were and not change once produced. Currently, SDN provides a data network and a control plane, which provides a powerful and flexible network [5]. However, the critical problem with SDN is security. And scalability also seems to be a major issue. For various reasons, the security of these new more flexible SDN are not as adaptable or they have inherent limitations. For example, when security functions are applied at centralized controllers, there will be a potential bottleneck; but when security functions are positioned at network functions, they are hardly capable of controlling the entire network. At most, security functions have been programmed to function on the control flexibility of SDN; however, this does not always lead to strengthened protection. As a result, current security implementations cannot hold up to conventional security measures [5]. The controller is an important part of the SDN. It connects the upper bridge and the lower parts. The distributed controllers' architecture has been studied and implemented by researchers and industry workers alike, by such as HyperFlow and Onix. The primary attention is focused on the distributed control plane and how to execute a global network topology for the application plane. Although it improves scalability, it does not improve security [6].

Distributed denial of service (DDoS) attacks

One type of security attack that is highly critical at any stage for SDN is the distributed denial of data (DDoS) attacks. For example, the breakdown of only one control could destroy the whole network. A method some hackers use to create DDoS attacks is that they use a massive number of new, but short length traffic flows. This in turn will cause a malicious overflow of SDN switches. Unfortunately, the lack of smart planning and applications limit SDN usability, feasibility, scalability, and security in real-time. OpenFlow is the most common SDN in use today [7].

While many security issues could be resolved in SDN by decoupling the network control logic from the data plane, the key security issue is DDoS. This rapidly growing network threat is usually performed on a target system to make the SDN unavailable to others. SDN can easily detect threats, while at the same time due to deviations in essential architecture and changes to basic design entities pose a critical DDoS threat to SDN [8]. Although SDN is evolving rapidly, Network Service Providers are implementing it because it is flexible, performance-ready, can be rapidly deployed and has good scalability, and for its centralized control plane and dumb switch devices, however, for all its benefits, SDN employs considerable threats. Therefore, a threat model is necessary for SDN. A threat model can explain how an adversary can compromise the network; a proper understanding of the SDN will develop better SDN protocols and assist with fool proof SDN debugging [4]. Therefore, the key problems and challenges with SDN and DDoS are indicated in the following chart.

Need for a distributed response at many points in the Internet
Lack of detailed attack information
Lack of defense system benchmarks
Difficulty of large-scale testing

Table 1: Challenges of SDN in DDoS [11]

Host-based intrusion detection system (HIDS)

Modern proliferation of social media has led to abundant information misuse within companies. To challenge this problem, local, internal inspections created by security experts have been known to assist in the solution. Host-Based Intrusion Detection System (HIDS), a technique which allows users to identify security risks at the endpoints, or individual hosts, combines HIDS and SDN to identify security risks. In both enterprise and virtualized networks, HIDS combines with SDN to enhance system security and, vital to the operational architecture, SDN introduces new security capacities. SDN software security provides protection against real-time attacks, provides access to legitimate users, and provides counter-attacks when necessary [9].

With all SDN connected to OpenFlow and HIDS network, a testable network is opened with an SDN-controlled network, constructed with multiple hosts, OpenFlow Enabled Switches, and a Floodlight Controller all which created the OSSEC Network when linked together (Open-Source Security) [9, 10]. For Cloud service providers, various network service options (e.g., bandwidth, safety, service quality, or reliability), require that the network architecture has flexibility as denoted by Network Function Virtualization (NFV). However, in traditional networks which have closed network equipment such as routers or switches, they may have the following drawbacks: software or hardware too tightly shut; network protocols are integrated into the devices and are too complicated; almost all devices are manufacturer-proprietary, meaning it is difficult to change them or update them. Since SDN is considered best practice, the goal will be to study how HIDS and SDN using OSSEC can reduce security risks for network users [9,10].

Cloud computing and software-defined networking

To reduce the level of threat against the network, an SDN uses novel techniques. Prior to any cyberattack the current network will most likely scout for impending attacks. Otherwise, without proper scouting, the network will probably fail if not scouted properly. Ransomware, botnets, and malware have the most negative effects against the networks. In SDN, a Moving Target Defense (MTD) can cause the perceived location of the network assets to shift continually [11]. A Random Host Mutation (RHM) is just one type of IP mutation of critical services. This makes it difficult if not impossible for malware to find assets. The RHM changes mutations frequently giving malware only a brief amount of time to access and take over the network assets. The MTD associated with SDN is meant to cause difficulty for malware to locate network assets [12].

The characteristic features of Cloud computing distribution make it susceptible to DDoS attacks. However, recent advancements in SDN have improved the likelihood of defeating DDoS attacks in Cloud environments. Several options of SDN make it highly likely that DDoS can be defeated: capability for software-oriented traffic investigation; dynamically updating forwarding rules; network global dimension; and the centralized point of control [12]. However, researchers have also discovered that a Fuzzy Self-organizing maps-based DDoS (FOSMDM) is extremely suitable and designed for defeating DDoS attacks in the Cloud. FOSMDM is a Cloud-based neural network which replaces conventional neurons by updating fuzzy rules. Software-oriented traffic investigation is used and is 94% more accurate than conventional methods [13].

DDoS attacks can cause many problems in the network. By causing a bottleneck, information is not allowed to flow in the normal channels, or compromised hosts on the network can send massive amounts of damaged data to individuals on the network. When these attacks occur, they do not allow information to flow smoothly, they can completely exhaust processing abilities, bandwidths of services, and networks causing a huge imbalance in the system, which may cause data loss, may compromise security, or any number of problems [14]. Individuals, businesses, and networks are affected by attacks on SDN. Because cyberattacks can come at any time, being prepared is key to defeating those criminals who would steal data, abuse networks, steal cybercoins, etc. Finding a suitable decision for a solution is critical to protecting data and security from terrorists, thieves, identity thieves, etc. [13].

Literature support

SDN improves network performance, provides better network control, and provides an area for innovation. However, despite these benefits, SDN is still in its early stages of development and has a few challenges and hurdles to overcome. SDN also has centralized control which makes it easier to identify a single point

control. To meet the growing needs of the numerous customers of SDN, it must be designed and operated to meet the requirements of growing users. A controller must always be available day or night for use by switches. Table 2 indicates how literature for SDN should be sorted in a review of literature to improve upon some challenges or innovations [15].

SDN Challenges	Network Design	Scalability
		Fault-tolerance
		Flexibility
		Elasticity
	Network Implementation	Integration with traditional networks
		Resource management
		Virtualization
	Network Performance	Latency
		Efficiency
		Consistency
		Traffic measurements
	Network Verification	Hardware testing
		Debugging
		Security

Table 2: Classification of SDN literature according to SDN Challenges [14].

Scalability, manageability, security, and availability are the key challenges of SDN. A network that is not flexible enough to handle the complications that arise can become a huge hurdle to manageability and security. SDN is flexible enough for staff to maintain the complexities and handle any security challenges [15]. Traditional security tools like firewalls and intrusion detection systems, are specialized to deal with a certain type of security threat and they are created together to compose a combined security prevention protocol. On the other hand, these tools will not fit in SDN, most tools are specifically designed and cannot be used by elements other than what they are designed for, and there is no interface on SDN or take advantage of its benefits. SecControl, proposed to identify real-time security threats, generate real-time reactions, and adjust network behaviors, accordingly, has been introduced by researchers to bridge the gap between traditional and SDN networks. This practical security system can provide strong security available in traditional networks with the flexibility of a an SDN [5].

DDoS attacks are attacks of availability. They can lead to massive interruptions in service, they can target specifically the network infrastructure, therefore, leading to the necessity for a complete overhaul in security measures for the current levels of networks to prevent severe peril. A crippled device, or bandwidth, or broken servers and storage can result in a lack of adequate security. Reports indicate many criminals hack medium to large organizations for their data. An essential solution is SDN networks where centralized control logic, software-enabled traffic monitoring, and a dynamic update of flow allow SDN to detect DDoS effectively and quickly before damage can be done. SDN has an architecture, and various DDoS attacks are categorized. However, the threats to SDN must be classified according to layer to prevent complications. Finally, an information distance-based flow discriminator framework has been proposed, which should address the DDoS attacks based on the SDN networks [8].

With the advancement of mobile technology today, it is also important to consider 5G and 6G abilities. Researchers have found that 5G services will offer the public a more dedicated and advanced line for mobile and wireless use. However, security, trust, and privacy are the three main areas which must be dealt with first. Therefore, researchers have proposed a dedicated 5G SDN network with an SDN-based integrated security network for the Internet of Radio Light (IoRL). IoRL is following 5G networks. For example, one type of attack which can be prevented is the DDoS [16].

Study methods

The approach for this study is based on using SDN, OpenFlow enabled switches, and Floodlight controllers to modify and set up an HIDS network using OSSEC and SDN to prevent or reduce any DDoS attacks. The researcher will run a testable SDN-controlled network, constructed using multiple hosts, OpenFlow enabled switches, and Floodlight controllers. This network will be linked to an OSSEC-HIDS network, executed in a server-agent architecture. This will foster OS independence and scalability. The system's effectiveness will be evaluated by the following: alert density, file integrity check frequency, rootkit detection status, and log monitoring workload. With an expected workload of approximately 550 events per second (EPS), results will show approximately a 0.5564 from log table generation to flow table update, using Floodlight [9].

Once a log has been decoded, it can be arranged that rules are applied to retrieve a specific dataset. Therefore, in this experiment,

the log rules need to match the authentication log. Active response is also technically separated into two elements within OSSEC: commands and configuration. This experiment defines the executable command in Linux [9,16]. Physical switches are used instead of virtual switches to represent a more hands-on and realistic approach to the experiment. To ensure accurate timing, a timestamp is used on the log and flow table update. All tests result in accuracy reporting of 94% greater than that of traditional security alerts or current SDN alerts [9,17].

In addition to the above methods, Big Data analytics will be used to analyze various data. Big Data analytics provides a 360-degree view of the system and facilitates real-time processing, which is critical for intrusion detection. A mix of anomaly-based intrusion detection and signature-based intrusion detection will also be used. Specifically, anomaly-based intrusion detection analyzes datasets, and if the results deviate much from normal then immediately intrusions are identified. Signature-based intrusion detection analyze features of specific attacks or intrusions.

Conclusion

Security is probably the most critical issue to be discussed among Internet users. With thieves who want to steal data, money, ransom data, and perform other malicious work, having high-level security and a highly functioning network is imperative today. With SDN, both can be achieved. Although security is an issue currently for SDN, it is a new concept and evolving daily. It is critical that researchers keep striving to make data and other information more secure on the Web. The most common cause of attacks and most dire are the DDoS attacks which can cripple an entire network.

Acknowledgement

The authors would like to thank Technology and Healthcare Solutions for support.

Conflict of Interest

Any financial interest or any conflict of interest does not exist.

Bibliography

1. Wang Shen., *et al*. "Novel architectures and security solutions of programmable software-defined networking: a comprehensive survey". *Frontiers of Information Technology and Electronic Engineering* 19.12 (2018): 1500-1521.

2. Benzekki Kamal., *et al*. "Devolving IEEE 802.1 X authentication capability to data plane in software-defined networking (SDN) architecture". *Security and Communication Networks* 9.17 (2016): 4369-4377.

3. Benzekki Kamal., *et al*. "Software-defined networking (SDN): a survey". *Security and Communication Networks* 9.18 (2016): 5803-5833.

4. Krishnan Saravanan and John Joel E Oliver. "Mitigating DDoS Attacks in Software Defined Networks". 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019: 960.

5. Wang Li and Dinghao Wu. "Bridging the Gap Between Security Tools and SDN Controllers". *EAI Endorsed Transactions on Security and Safety* 5.17 (2018): 1-16.

6. Zhong Hong., *et al*. "SCPLBS: a smart cooperative platform for load balancing and security on SDN distributed controllers". *Peer-to-Peer Networking and Applications* 12.2 (2019): 440-451.

7. Conti Mauro., *et al*. "Lightweight solutions to counter DDoS attacks in software defined networking". *Wireless Networks* 25.5 (2019): 2751-2768.

8. Sahoo Kshira Sagar., *et al*. "Toward secure software-defined networks against distributed denial of service attack". *The Journal of Supercomputing* 75.8 (2019): 1-46.

9. Goodgion Jonathan and Barry Mullins. "Active Network Response Using Host-Based IDS and Software Defined Networking". ICMLG 2017 5th International Conference on Management Leadership and Governance. Academic Conferences and publishing limited (2017): 469-478.

10. Zhang Heng., *et al*. "A survey on security-aware measurement in SDN". *Security and Communication Networks* (2018): 1-14.

11. Shu Zhaogang., *et al*. "Security in software-defined networking: Threats and countermeasures". *Mobile Networks and Applications* 21.5 (2016): 764-776.

12. Mayer Samuel., *et al*. "Look Again, Neo: A Software-Defined Networking Moving Target Defense". International Conference on Cyber Warfare and Security. Academic Conferences International Limited, (2018): 602-610.

13. Pillutla Harikrishna and Amuthan Arjunan. "Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing". *Journal of Ambient Intelligence and Humanized Computing* 10.4 (2019): 1547-1559.

14. Cheng Haosu., *et al*. "A Compatible OpenFlow Platform for Enabling Security Enhancement in SDN". *Security and Communication Networks* (2018): 1-20.

15. Saraswat Surbhi., *et al*. "Challenges and solutions in Software Defined Networking: A survey". *Journal of Network and Computer Applications* 141 (2019): 23-58.

16. Cabaj Krzysztof., *et al*. "Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System". *Security and Communication Networks* (2019): 1-22.

17. Festijo Enrique., *et al*. "Software-defined security controller-based group management and end-to-end security management". *Journal of Ambient Intelligence and Humanized Computing* 10.9 (2019): 3365-3382.

Volume 1 Issue 2 December 2019