INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

A Novel Pre-shared Information Defense Mechanism For Spoofed IPAttack in SDN - A Review

Manisha Lalotra[*], *CSE Deptt., SSCET, Badhani,* manishalalotra21@hotmail.com

Meenakashi Sharma, *CSE Deptt., SSCET, Badhani*

Gurjeet Kaur., *CSE Deptt SSCET, Badhani*

Abstract*—The software defined networks are being used in many scenario where the ordinary Or traditional network management becomes the real problem. Such networks are defined or managed with the SDN platform, which is used as the network programming rather than the network configuration. The problem of user legitimacy is a big issue in the cloud platforms. The user legitimacy assurance is quite important to protect the cloud platforms from several types of attacks. The user legitimacy assurance must be performed on two given events, one is pre-setup, second is post-setup. The existing models incorporate the post-setup phase authentication only, where the pre-setup phase is left immature, where the hackers can easily attack over. In this paper, we are proposing the model for the security of cloud by user legitimacy assurance during the pre-setup phase with the use of pre-shared information in the form or RUID (rigid user ID), which is provided to the user during the registration. The RUID will add the new layer of security by mitigating the threat of user session hijacking, which will make the cloud infrastructure highly secure in comparison with the existing models.

***Keywords*—SDN, CDN, CDNi, ALTO, DDoS Attack, Selective Jamming.**

I. Introduction

Software defined networking model, is a data plane (packet forwarding) and management plane work with the device. However, the control plane (forwarding decisions) combine data packets into a single more coherent and effective way in a central location, that can be an Open Flow controller, or a hypervisor manager. The controller takes the information about packets arriving at the port and makes a decision a how to process the packets. This decision can be make on the basis of first packet, then the controller process all of the SDN devices in the path by forwarding information for subsequent packets that is called a "flow".

1.1MODELS

There are two models of Software Defined Networking:

- Open Flow Model
- Network Virtualization.

The Open Flow is an open standards protocol maintained by the ONF. It uses the software program called a controller to configure the data planes on the devices by which it can controls the data packets.

\

The other model Network Virtualization for SDN comes under the set of Network Virtualization. That is called hypervisor environments. In this type of environment, the control plane is generally establish as a virtual machine or in the hypervisor manager, and the data plane is a module loaded onto each hypervisor host.

Network security remains a major challenge in the Cyberspace. The amount of endangerments which could attack a network is a tough call. Worms, SPAM, Denial-of-Service attacks or Botnets are only a small piece of threats occurring every minute thousand fold in networks around the globe. From inside the network it is necessary to detect such an offense otherwise no mitigation is possible. In addition to these two necessities a network can try to obscure their resources and services to defend attacks. The latter is a more complex task since a service must be public available, but yet hidden for attackers at the same time. To face all these issues a holistic solution has to be implemented, which takes into account current vulnerabilities of connected systems as well as policies that regulate access and quality of service. Software defined networking (SDN) can support these ideas by providing a logical centralized view and possibilities to steer specific types of traffic in an easy way. Current approaches lack of a closed view over a part of the network and don't take into account networks and services nearby.

To overcome these issues we propose a solution which benefits from existing approaches in traditional networks like Intrusion Detection Systems (IDS), vulnerability scanning, network policy enforcement or feeder- acted identity management to mention only part of them, and combines these with the advantages of SDN to react in a comprehensive way to fulfill policies, defined requirements and keep the offered service alive while under attack. This can't be done by a single SDN controller even if highly accurate monitoring data is available. Our solution tries to distribute several agents which are aware of the high level goals of the policy administrators as well as the security concerns caused by monitoring data, e.g. IDS and security regulations from the respective cloud administrator. Afterwards these agents cooperate together to ensure the compliance of the high level goals, that result in various low level goals from local devices or administrators in the observed area of each agent. Since such a complex solution can't be established immediately solutions to implement such a system step-by-step have to be developed. Our main goal is to investigate how traditional monitoring and observation data can be used as a basis for forwarding decisions in SDN enabled networks while ensuring security and service quality concerns.

When dealing with cloud scenarios special requirements arise in respect of security. Most security concepts work very well on common data-centre hardware and widely used software solutions. Nevertheless these concepts are also valid in cloud scenarios, but rather inefficient and error-prone, e.g. enabling a host- based firewall on every virtual machine in the cloud requires much more resources than blocking or permitting traffic on the virtual switch every virtual machine is connected to. Using SDN as a new promising network paradigm, opportunities arise to merge service requirements, policies and security issues that define precise goals and are implemented without further manual interaction. Possible input values are manifold and have to be translated into convincing high level goals, which themselves cause a couple of low level goals and decisions, being aware of the corresponding context where they originated. To define such complex dependencies and hierarchies of service requirements, policies and security issues of existing approaches have to be adapted to interact briefly together.

The complexity of this approach leads to a more detailed subdivision. SDN (Software defined Networking)in the explosion of cloud services, mobile services and always connected lifestyle, transforming business and education around the world. The organizations are continue to design their network under client/server model. But in now days application world is changed SDN change all the things I will automatically meet to change and business needs .but the configuration of network is not changed it s time consuming, error, and Manual process that can take days or week to complete and also suffer from vendor lock-in because configuration and control of network traffic is handle by independently by each vendor. But With the help of SDN the data centre are virtualized and network service provider can be automatically created and deleted as the business needs. In simple ways router and the switches consist only two plane control plane and data plane. The control plane determines the route of data packets and the data plane is part of network handle the traffic of network .But in case of SDN there is a difference-

\

SDN Architecture

SDN separates the network into three layers—application, control, and data.

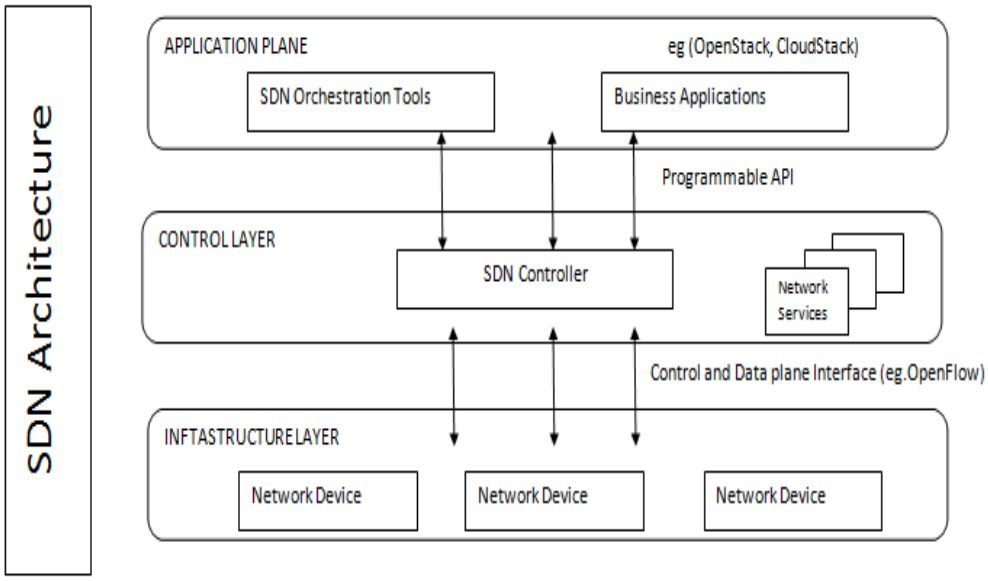

Figure 1: Architecture of SDN

- **Application Plane-** SDN applications present in the application plane and communicate with their requirements via an application programming interface (API). Developers can write their applications that control the logical network, and network operating system take care of the detail work. It may be network applications, cloud, or business applications. All these are handle by the application plane.

- **Control Plane-**In SDN, the control plane is logically centralized and decoupled from the data plane. The SDN controller translates the application requirements and controls the SDN data paths, while communicating with SDN applications. Decisions are made according to the current view of the entire network rather than within the limited visibility of each network hope, as routers do today. The SDN controller is essentially a network operating system that constructs a logical map of the network to services or applications that are implemented on top of it.
- **Data Plane-**The SDN controller controls the SDN data paths, which simplifies resource allocation and enables quality-of-service guarantees from end to end. The SDN data path is the logical network device that forwards the actual traffic.

\

SDN Based Security-

- **SDN role in security**-SDN will enhance network security and access control. This technology offers a higher level of visibility, which results in more granularities in packet analysis, network monitoring and traffic engineering. Centralized control can allow advanced network policy implementation and enforcement by routing individual flows to specific devices .The centralized control will result in security defined routing.
- **SDN in cloud-**SDN will be used to provide Network as a Service (NAAS). Cloud computing allows provisioning of resources on demand. Network security in cloud provider networks differ from its counterpart in traditional networks, since their networks include much more dynamics than traditional networks. Whereas it is possible in traditional networks that a single administrator or a small group of network administrators can change a specific routing table entry or access control lists to change the behavior of the network, traffic flow or give access to relevant resources, this is not feasible in highly dynamic networks, especially in cloud environments where virtual machines and computing power are allocated and withhold in short time periods without manual interaction. Another security drawback in cloud environments is the variety of software and operating systems, which are not under control of one organization and therefore lead to new attack scenarios, like establishing access through an unsecured system to a previously selected target, which runs inside the same cloud environment.
- To prevent such security endangerments in a cloud environment, access and security policies have to be deployed immediately after a system is set up and redefined after every change of the system, e.g. configuration changes through the systems' administrator, updates or service modifications. An approach has to be aware of all provided services and vulnerabilities of a system running in the respective cloud. This can be ensured through a requirement for an initial input during the setup process of a new system, which includes relevant system information, but it has to be updated continuously. A central manager has to be aware of all properties of a system at every point in time. Following this approach policies can be applied on demand taking into account permanent and temporary requirements for accessing and securing recently deployed systems. The major challenges in this environment are the high dynamics in deploying and displacing services which includes provisioning of resources, especially network enabled resources.
  - **a) Software as a Service - SaaS**: SaaS can be separated into a diversity of security issues. This paper aims to give a short overview without going into details. Network security issues in this delivery model is often provided via commonly known SSL encryption endpoints depended on the cloud provider, e.g. in the case of Amazon Web Services (AWS) significant protection against traditional network security issues, such as packet sniffing, MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, is provided. The data location problem, which is mostly tackled if business data is outsourced in the cloud, is addressed in [5]. Data integrity and data segregation is investigated in almost all cases via generally accepted techniques (e.g. XML based APIs, SOAP and REST services with transactions support and data validation techniques). On behalf of data access and authentication/authorization for accessing services, various approaches.
  - **b) Platform as a Service - PaaS:** PaaS tries to give control to consumers that build applications on platforms. So the provider should be aware of the security below the application level (e.g. host and network intrusion prevention). Most applications leverage the Enterprise Service Bus (ESB). In these cases the ESB has to be secured directly.
  - **c) Infrastructure as a Service - IaaS:** Customers using IaaS have to be aware of all possible security issues of their systems, except a security lack in the hypervisor of the environment is out of their scope. Since the rapid emergence of virtualization of everything in information society, the control over data regardless of its physical location raised outmost interest whereas the question of responsibility (cloud provider or consumer) is not clearly answered and differs between all aforementioned service models.

II. LITERATURE SURVEY

The IPv6 based approach [5] for the operations and scenarios (Tsengp Chia-Wei et. al. 2014) has been presented for the IPv6 deployment in the integrated software defined networks (SDN). The combination of SDN with the IPv6 has been proposed for the creation of a smarter and reliable network. The major aspect of this paper lies in the co-existence of the IPv4 and IPv6 technologies alongside. For the wireless network management the software defined networks has been used as defined in the [4]. Alejandro De Ganteet. al. have given the concept of smart wireless sensor networks, where the SDN is used to take on inherent problems in WSN management. The network base station has been utilized as the controller unit for the SDN to manage the whole WSN architecture. The useful results are found SDN into WSNs could help in tackling some of the difficult problems in WSNs such as energy saving and network management. The network has been analysed in the some of the studies of for their security management [2] and [6]. M. Belyaevet. al. has worked on the distributed denial of service (DDoS) attack mitigation in the SDN environments. The DDoS attack is proved to the dangerous every year as the number of DDoS attacks are on the rise [2]. The financial studies on IT infrastructure show that the losses caused due these attacks have also surged

\

drastically in the recent years. In [6], the packet flow count method has been used to detect the traffic anomalies in the SDN environments. The granularity measurement method has been utilized for the flow count which is analysed for the purpose of anomaly detection along the temporal and spatial domain [6]. In both, [2] and [6], the survival time of the SDN based network defending system has been improved against the various kinds of attacks on the networks. DezeZenget. al. [6] have given the study about the realization of the software defined networks. The authors have given the concept of SDNs and have outlined the pioneering and important methods in the timeline of SDN architecture development. With the advancement of existing information technologies such as cloud computing, OTAP, SDN, SDR and FPGA, that SDSNs are not only necessary but also inevitable in the next-generation sensor networks. The source based forwarding has been also explored in the SDN-based network architectures. The source routing mechanism [3] encourages the use of alternative hops in the SDN-based WAN deployment. The internet or WAN is widely managed between the different autonomous systems. Mainly the data is exchanged between these autonomous systems to form the major internet construction. The source based routing has been proposed to solve the problem of the network convergence time and to control the dimension of the controller placement problem. In [5], the source routing has been utilized as described in [2] with a little improvement for the IPv4 and IPv6 based inter-domain and intra-autonomous system routing. In [1], the efficient defense mechanism based on ALTO server has been proposed for the spoofed IP attack, which is inspired from the [2] and [6] in the cloud based SDN environment similar to the description presented in [5]. The use of ALTO server has been profoundly encouraged for the implementation of security architecture against the spoofed IP based attacks. The SDN based CDNi network has been enabled with the mapping module for the very big networks to facilitate the summarized view of the network routines. The ALTO server based SDN for CDNi [1] has been made capable to detect the DDoS attack launched by the attackers with spoofed IPs. An encrypted combination of IP address and Partition ID (PID) has been provided and saved by ALTO like servers which map the entire Networks. In [5], the algorithm has been created as an application for the SDN controller to detect spoofed IP address by the SDN switches.

Comparison Table: Difference between the SDN over CDNi for Packet Spoofing and DDoS attacks

PROPERTY	IP SPOOFING DEFENCE	DDOS DEFENCE
Technique Name	Nishat I Mowla "An Efficient Defense Mechanism for Spoofed IP Attack in SDN based CDNi"	Nishat-I-Mowla "Multi-Defense Mechanism against DDoS in SDN based CDNi"
Protects Against	IP Spoofing attack	DDoS attack
Architecture Used	ALTO server for CDNi security data management	ALTO server for CDNi against flooding attacks
Security Mechanism	UID table to filter the unauthorized users	MIB (management information base) to filter authorized users
Detection Mechanism	IP detection	Path Map based IP detection
Propagation Medium	Secure code propagation in the packet header	Assess the ingress traffic on switches against the path map

III. CONCLUSION AND FUTURE WORK

The cloud computing platforms are also considered the enterprise networks and are highly prone to several forms of attacks, critically packet flooding attacks. The SDNs can provide stronger security for the cloud platforms. The trusted or verified sources in the whole network can kept in the black lists or white lists, which make it easier to protect the cloud sources from the malicious nodes or attacker nodes. The importance of data filter arises when the data coming from the non-trusted sources lowers the performance of the cloud clusters. In order to protect such problem, the existing model has been designed to mitigate the malicious nodes from the cloud platform. The malicious nodes are detected on the basis of their unique ID saved in the node information table called "mark map". The existing model is not equipped to protect against any attacks during the pre-setup phase. The pre-setup phase is the initial phase of the communications, where the two nodes setup a connection between them. In order to mitigate such problem, we are proposing the use of rigid UID (RUID), which comes pre-embedded in the client nodes, or obtained during the registration phase. This is termed as rigid UID, because it can be not be altered, generated or duplicated by any means of data forgery. This will create a stronger system for the higher level of security for the cloud platforms. Also the encryption model used in efficient as there has been used a weaker fiestel network based encryption, which must be secured in order to minimize the effect of the

\

attacks on the cloud platforms. In the proposed model, we will use a stronger encryption algorithm with multi-factor data hiding for the robustness of the security.

The software defined network can handle the whole user membership security service over the cloud platforms using the centralized database saved with the pre-shared information entries and their activity status. The pre-shared security information which has been provided to some of the user is activated or saved with the software defined network module over cloud platform. The clients will be required to share the pre-shared information in the encrypted form during the initial setup of communication channel. Only if the pre-shared information will be verified, the access will be granted to the nodes, otherwise the client node will be denied the connection. The proposed model will then follow the sharing of the RUID (rigid user ID) during the pre-setup and post-setup phases of the communication. In this way, we will secure the cloud platform by using it with the SDN.

The proposed work will be reviewed in order to refine the algorithm structure in order to mitigate the future threats of the algorithm. The proposed model will be then simulated using the simulation environment using the MiniNet or EstiNet simulator, which are the primary options for the software defined network simulation. The simulation environment will configured with all of the essential input and output parameters for the better evaluation of the experimental results. After completing the simulation, the proposed model will be tested thoroughly and compared with the existing counterparts to evaluate its performance and the possible improvement in the performance.

The proposed model has been designed to work over the software defined network (SDN) for the content delivery networks (CDNi). The proposed model is a pre-shared information based security model which is used for the user legitimacy assurance of the cloud based applications or cloud platforms itself. The pre-shared information based security model is the most efficient feature to protect the online resources from several forms of attacks on the cloud networks. The proposed model simulation should be performed using the MiniNet or EstiNet simulators used for the software defined network simulation. In the future, the proposed model can be enhanced using the more efficient ways of security for the SDN based cloud platforms.

REFERENCES

1. Mowla, Nishat, InshilDoh, and KijoonChae. "An efficient defense mechanism for spoofed IP attack in SDN based CDNi." In *Information Networking (ICOIN), 2015 International Conference on*, pp. 92-97. IEEE, 2015.
2. Belyaev, M., and S. Gaivoronski. "Toards load balancing in SDN-networks during DDoS-attacks." In *Science and Technology Conference (Modern Networking Technologies)(MoNeTeC), 2014 First International*, pp. 1-6. IEEE, 2014.
3. Soliman, Mourad, BiswajitNandy, IoannisLambadaris, and Peter Ashwood-Smith. "Exploring source routed forwarding in SDN-based WANs." In*Communications (ICC), 2014 IEEE International Conference on*, pp. 3070-3075. IEEE, 2014.
4. De Gante, Alejandro, Mohamed Aslan, and Ashraf Matrawy. "Smart wireless sensor network management based on software-defined networking." In*Communications (QBSC), 2014 27th Biennial Symposium on*, pp. 71-75. IEEE, 2014.
5. Tseng, Chia-Wei, Sheue-Ji Chen, Yao-Tsung Yang, Li-Der Chou, Ce-KuenShieh, and Sheng-Wei Huang. "IPv6 operations and deployment scenarios over SDN." In *Network Operations and Management Symposium (APNOMS), 2014 16th Asia-Pacific*, pp. 1-6. IEEE, 2014.
6. Zhang, Ying. "An adaptive flow counting method for anomaly detection in sdn." In *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*, pp. 25-30. ACM, 2013.
7. Zeng, Deze, Toshimasa Miyazaki, Song Guo, Tsuneo Tsukahara, JunjiKitamichi, and Teruaki Hayashi. "Evolution of software-defined sensor networks." In *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on*, pp. 410-413. IEEE, 2013.
8. Sezer, Sakir, Sandra Scott-Hayward, Pushpinder-KaurChouhan, Barbara Fraser, David Lake, Jim Finnegan, NielViljoen, Mary Miller, and NeerajRao. "Are we ready for SDN? Implementation challenges for software-defined networks." *Communications Magazine, IEEE* 51, no. 7 (2013): 36-43.
9. Scharf, Michael, Thomas Voith, W. Roome, Bob Gaglianello, Moritz Steiner, Volker Hilt, and Vijay K. Gurbani. "Monitoring and abstraction for networked clouds." In *Intelligence in Next Generation Networks (ICIN), 2012 16th International Conference on*, pp. 80-85. IEEE, 2012.
10. Monsanto, Christopher, Joshua Reich, Nate Foster, Jennifer Rexford, and David Walker. "Composing Software Defined Networks." In *NSDI*, pp. 1-13. 2013.
11. Tootoonchian, Amin, Sergey Gorbunov, YasharGanjali, Martin Casado, and Rob Sherwood. "On controller performance in software-defined networks." In*USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services (Hot-ICE)*, vol. 54. 2012.
12. Shin, Seungwon, Phillip A. Porras, VinodYegneswaran, Martin W. Fong, GuofeiGu, and Mabry Tyson. "FRESCO: Modular Composable Security Services for Software-Defined Networks." In *NDSS*. 2013.

\

13. Kreutz, Diego, Fernando Ramos, and Paulo Verissimo. "Towards secure and dependable software-defined networks." In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 55-60. ACM, 2013.
14. Reitblatt, Mark, Nate Foster, Jennifer Rexford, and David Walker. "Consistent updates for software-defined networks: Change you can believe in!." In*Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, p. 7. ACM, 2011.
15. Nascimento, Marcelo R., Christian E. Rothenberg, Marcos R. Salvador, Carlos NA Corrêa, Sidney C. de Lucena, and Maurício F. Magalhães. "Virtual routers as a service: the routeflow approach leveraging software-defined networks." In*Proceedings of the 6th International Conference on Future Internet Technologies*, pp. 34-37. ACM, 2011.
16. Kim, Hyojoon, and Nick Feamster. "Improving network management with software defined networking." *Communications Magazine, IEEE* 51, no. 2 (2013): 114-119.
17. Jain, Sushant, Alok Kumar, SubhasreeMandal, JoonOng, Leon Poutievski, Arjun Singh, SubbaiahVenkata et al. "B4: Experience with a globally-deployed software defined WAN." In *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 3-14. ACM, 2013.
18. Channegowda, Mayur, Reza Nejabati, and DimitraSimeonidou. "Software-defined optical networks technology and infrastructure: Enabling software-defined optical network operations [Invited]." *Journal of Optical Communications and Networking* 5, no. 10 (2013): A274-A282.
19. Mehdi, Syed Akbar, Junaid Khalid, and Syed Ali Khayam. "Revisiting traffic anomaly detection using software defined networking." In *Recent Advances in Intrusion Detection*, pp. 161-180. Springer Berlin Heidelberg, 2011.
20. Qazi, ZafarAyyub, Cheng-Chun Tu, Luis Chiang, Rui Miao, VyasSekar, and Minlan Yu. "SIMPLE-fyingmiddlebox policy enforcement using SDN." In *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 27-38. ACM, 2013.
21. Hassan Ali-Ahmad1, Claudio Cicconetti2∗, Antonio de la Oliva3 ." An SDN-based Network Architecture for Extremely Dense Wireless Networks". Future Networks and 2013 - ieeexplore IEEE.org
22. N Mowla, I Doh, K Chae . "Multi-defense Mechanism against DDoS in SDN Based CDNi". Innovative Mobile and Internet 2014 - ieeexplore.IEEE.org

\

