THE NOVEL METHOD OF PROVIDING SECURITY IN D-SDN THREATS AND COUNTERMEASURES

[1]Mrs.P.R.RUPASHINI, [2]Mr.LINGAM.M, [3]Mr.SRIVIGNESH.S, [4]Mr.VIGNESH.K,[5]Mr.VIGNESH.S
[1]Assistant professor, [2]student, [3]student, [4]student, [5]student
Department of Computer Science, United Institute of Technology, Coimbatore-20, India.

ABSTRACT-Software Defined Networking (SDN) is an leading architecture that is dynamic manageable, cost-effective, and adaptable, making it ideal for high bandwidth, dynamic nature of today's application network intelligence is (logically) centralized in software based SDN controllers. The cleverness centralization has its own disadvantage when it comes to security, SDN architecture may enable facilitate or enhance network related security application due to the controller's central view of the network, and it's capacity to reprogram the data plane at every time.so we propose Decentralize-SDN, D-SDN control distribution by defining of controller that can match an internets organizational and administrative structure. D-SDN, control distribution is based on a hierarchy of MC's and SC's which can also be used to improve control plane availability and fault tolerance. D-SDN is that it consolidates security as integral part of the framework and its underlying protocol's.

Keywords- SDN, D-SDN, MC, SC, DDOS, POX.

---

1. INTRODUCTION

Software-defined networking (SDN) technology is a novel approach to cloud computing that facilitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring. SDN is meant to address the fact that the static architecture of traditional networks is decentralized and complex while current networks require more flexibility and easy troubleshooting. SDN suggests to centralize network intelligence in one network component by disassociating the forwarding process of network packets (Data Plane) from the routing process (Control plane). The control plane consists of one or more controllers which are considered as the brain of SDN network where the whole intelligence is incorporated. However, the intelligence centralization has its own drawbacks when it comes to security, scalability and elasticity and this is the main issue of SDN.

The SDN Architecture is, directly programmable, centrally managed, programmatically configured, Open standards-based and vendor neutral,

Figure 1.1 Overall Architecture for Security in D-SDN Threads and Countermeasures

2. EXISTING SYSTEM

Existing approaches with the advancement of research into SDN, the security issues of SDN attract more and more attention from manufacturers and operators. In this section, we will describe in detail the main security threats and countermeasures that have been presented. According to the above-presented SDN architecture and related security analysis, we divide the threats and corresponding countermeasures into three categories based on which layer of the SDN architecture contains corresponding attack target, i.e., the forwarding layer, the control layer and the application layer.

The SDN architecture's characteristics impact on security. Compared to traditional network architectures, security threats of SDN will be even more concentrated, as opposed to the dispersion seen in the network elements of traditional networks. Therefore, because of its design nature, SDN has security advantages and security defects.

It advantages include:

- Effective monitoring of abnormal traffic
- Timely dealing with vulnerabilities

- On the other hand, the natural security defects of SDN include
- Vulnerable controller
- Risks caused by open programmable interface

2.1 DRAWBACKS OF EXISTING SYSTEM
Security:

- Attacks at Data Plane Layer
- Attacks at Controller Layer
- Attacks at SDN Layer (Application Layer)

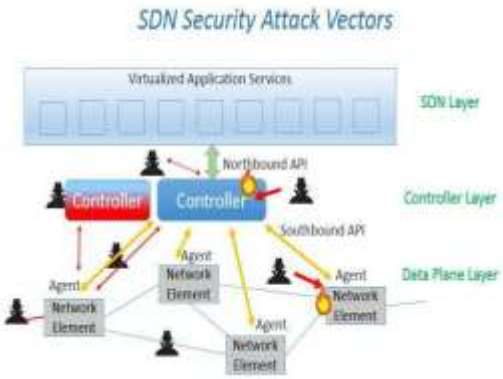

Fig 2.1 SDN Security Attacks Vectors

Centralized architecture of SDN based networks itself is a huge challenge. Other challenges of immature code base, lack of features, lack of support etc. are temporary disadvantages which will go away with time.

However, SDN based networks will always have a centralized architecture because you want to pull out the intelligence from the boxes and move it to an application on the controller. One controller manages the network. Becomes a single point of failure so you add clustering and HA support. Now 5 controllers function in a cluster to support a network. These 5 will only support anywhere between 200-2000 devices. As you add elements to the network you need to add more controllers. Now these different clusters need to work together to manage your network. So you keep on adding intelligence through other nodes which do not reside on the device. Internet/Networks inherently is distributed in nature. You take away the flavor of distributed architecture once you remove all the intelligence from these devices.

3. PROPOSED SYSTEM:
3.1 Advantages of Proposed System:

D-SDN method utilize and increases the resilience of our framework to attacks such as impersonation, man-in-the-middle and replay-attacks. It enables reasonably decentralized control through control delegation between different levels of the control hierarchy. Network capacity sharing, in which control decentralization enables nodes in an infrastructure-less network to connect to the Internet via other (connected) nodes, and public safety network (PSN) sketch that showcases control decentralization in emergency response services

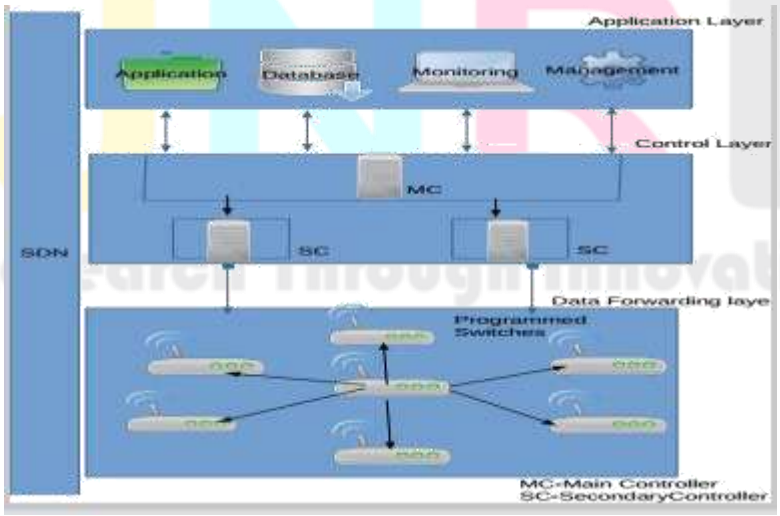

Fig 3.1 Architecture of D-SDN

3.2 Security

[1] Ubuntu's goal is to be secure "out-of-the box". By default, the user's programs run with low privileges and cannot corrupt the operating system or other users' files.

[2] For increased security, the pseudo tool is used to assign temporary privileges for performing administrative tasks, which allows the root account to remain locked and helps prevent inexperienced users from inadvertently making catastrophic system changes or opening security holes. Policy Kit is also being widely implemented into the desktop. Most network ports are closed by default to prevent hacking.

[3] A built-in firewall allows end-users who install network servers to control access. A GUI (GUI for Uncomplicated Firewall) is available to configure it. Ubuntu compiles its packages using GCC features such as PIE and buffer overflow protection to harden its software. These extra features greatly increase security at the performance expense of 1% in 32-bit and 0.01% in 64-bit.Ubuntu also supports full disk encryption as well as encryption of the home and Private directories.

3.3ADVANTAGES:

[1]Better User Interface: A much better interface with HUD which believes that everyone is not using a touch based monitor.

[2]Security: Due to the low usage ratio and emphasis on security it has a lower chance of being infected. (Used in nearly all the stock exchanges and big web giants such as Google so be pretty sure on that front)

[3]Centralized Software Repository: A windows store like app in which you can download and install apps without the hassle of opening the websites every time and adding new Repositories for software which can be updated together from one location.

[4]Command Line: A Supplement of the above with the environment the UNIX shell is also programmable making it easy to write programs for and interact with it. Anything that can be done with GUI can also be done here it has apps from media players (mpv) to download accelerators (axel). Resources: Ubuntu consumes lesser resources and thus is somewhat faster as compared to windows. This can also be used to revive older systems which cannot cope up with requirements that windows places on its users.

4. IMPLEMNTATIONS and RESULTS:

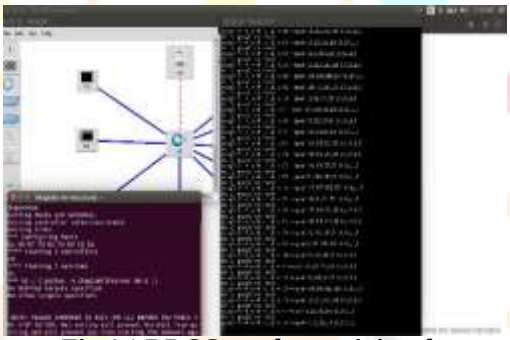

Fig.4.1 DDOS result on mininet host

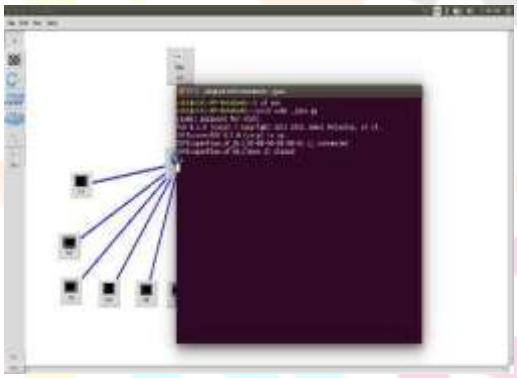

Fig.4.2 POX Controller

5. CONCLUSION:

As future work, envision new D-SDN based network services and applications, such as inter-domain routing, load balancing and monitoring. In proposed Decentralize-SDN, a general framework empowers a wide range of current as well as future network services and applications through the decentralization of the SDN control plane. D-SDN supports control distribution by defining a hierarchy of controllers in which main controllers can delegate functions to secondary controllers. In this work we have investigated the decentralization problem of SDN. In characterized correctness and optimality of forwarding rule installation policies. While the problem of finding an optimal correct installation policy is undecidable.

6. REFERENCES

[1] Jiafu Wan,Di Li, Athanasius Vasilakos, "Security in software defined Networking Threats and Countermeasures:, Mobile Networks and Applications January 2016 Impact Factor: 1.05 DOI:1007/s11036-016-0676-x

[2] D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann,"Logically centralized?: state distribution trade-offs in software defined networks," in Proceedings of the workshop on Hot topics in software defined networks. New York, USA: ACM, 2012, pp. 1–6.

[3] Dixit,A.,Hao,F.,Mukherjee,S.,Lakshman,T.,andKompella,R.Towardsan elastic distributed SDN controller. In Proceedings of the second ACMSIGCOMM workshop on Hot topics in software defined networking (New York, NY, USA, 2013), HotSDN '13, ACM, pp. 7–12.

[4] Shin S, Yegneswaran V, Porras P, Gu G (2013) Avant-guard: scalable and vigilant switch flow management in software-defined networks. In:Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp 413–424

[5] Wang H, Xu L, Gu G (2015) Flood Guard: a dos attack prevention extension in software-defined networks. In: 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp 239–250

[6] Lim S, Ha J I, Kim H, Kim Y, Yang S (2014) A SDN-oriented DDOS blocking scheme for botnet-based attacks. In: IEEE Sixth International Conference on Ubiquitous and Future Networks (ICUFN), pp 63– 68

[7] Lim S, Ha J I, Kim H, Kim Y, Yang S (2014) A SDN-oriented DDOS blocking scheme for botnet-based attacks. In: IEEE Sixth International Conference on Ubiquitous and Future Networks (ICUFN), pp 63– 68