Security challenges for software defined network deployment

Science, Computer Science

Overview

Software Defined Network (SDN) virtualizes your network to notional physical hardware network elements such as switches and routers. Using SDN you can manage your datacenter networking more effectively to meet the workload requirements. Networking policies can be executed perpetually, even as you deploy new and heavy workloads, or move workloads across the physical or virtual networks.

History of Software Defined Networking (SDN)

2009: An article was published by Nick McKeown which revealed his observations regarding Software Defined Networking. These observations stated that that in prior attempts to deploy a software defined network, it was assumed that the Current IP routing substrate was fixed and was tried to be programmed externally, including the routing protocols. Also the prior attempts of SDN defined the programming and control model beforehand. But to pick the right 32bit instruction set, Intel did not define Linux, Windows XP or VMware.

2010: In 2010, an article was published by Stanford University professors stating the limitations of SDN at that time period. The SDN at that current time did not specify how the applications should have interacted with the network. An application might have continued using the minimal socket API and viewed the network merely for inter-connection. The main question at the time was that how would applications interact with the network in a world where owners could add new functionality to the control plane. It was understood that SDN was still in its infancy.

2011: In an article published in 2011, it was said that the main challenges for SDN was making distributed control problem a logically centralized one that involved a common distribution layer. The article also said that it would take years to internalize and evaluate abstractions and even longer to adjust the software oriented culture. The authors also mentioned that they were in very early stages of an intellectual voyage.

2012: An article in 2012 illustrated all the bugs the authors had found during their testing with an SDN. They saw a race condition when they were installing switch flow entries and a controller logic error. Also they discovered a bug in the switch implementation. They tried to overcome the problems and bugs by algorithms in the proxy components of a prototype ndb (network debugger) to modify control messages.

2013: In 2013, a security survey of SDN was conducted which concluded with the results that many challenges existed for full scale carrier implementation of the SDN with one key area being security in SDN. There were increased potential for DoS attacks due to the centralized controller and flow-table limitation in network devices. One of the other issues is trust between applications and controllers, and controllers and network devices. They conclude that due to the nature of the centralized controller and the programmability of the network, new threats are introduced requiring new responses.

2014: In an article published by Fei Hu, SDN security is further elaborated. SDN created new targets for potential security attacks such as SDN controller and the virtual infrastructure. Also SDN introduces new methods but alongside them new target points such as the SDN controller and Open Flow network. Also there were issues with the routing loops which would make the packets never reach their final destination.

2015: In a 2015 article, authors explained how the control plane was susceptible to DDoS attacks where many compromised hosts distributed in the network may flood the network switches with packets at the same time. Since not all rules will be available in the switches' tables, many queries will be sent to the controller which ends up utilizing the controller's processing power which then causes actual queries to be delayed or eventually then be dropped.

2016: An article published in 2016 explained new threats to SDN as it evolved. Man-in-the-middle attacks were a common network intrusion method, the main principle of them was to insert an agent node between the source and the destination, and used to intercept communication data and tamper with it without being detected by the communicating sides. Specific attack methods of man-in-the-middle attacks include session hijacking and DNS spoofing etc.

2017: In an article which was published yester-year, the author elaborates that SDN is a logically centralized technology and the scalability, especially of the control plane (which is the SDN controller) scalability in SDN is one of the major problems that needs more attention. In this survey paper, it was also discussed about the scalability problems of controller/controllers in the SDN architecture.

2018: In an article published recently based on the security of SDN, all relevant assets are controlled not by a single entity but by various operators (including, in some cases, end users) who need to cooperate with each other. A dire consequence of this situation is that every element of the infrastructure can be targeted at any moment. In fact, this “ anything, anytime” principle is also inherited from some of the building blocks and application scenarios, such as the Internet of Things.