Prof. Dr.-Ing. habil. Falko Dressler
Data Communications and Networking – TKN

Technische Universität Berlin

Master's Thesis

Synchronisation of Distributed Intrusion Detection System via SDN

Firewall is well-known as the first layer of defense for your network. However, intruders developed new techniques to bypass the firewall and gain access to the network. Following, Intrusion Detection System (IDS) is introduced as a new layer of defense after the firewall to make the intruders' life more painful than ever.

The current volume of network traffic is on a scale that a single IDS which is developed based on the most accurate approach (Deep Packet Inspection) can not analyze it completely. The network specialists recommend the deployment of multiple instances of IDS across a network to increase the overall processing capability. However, the assignment of traffic to each IDS in a way that maximizes the utilization of the processing capacity is a big challenge. Let's take a look at an example to make the challenge more clear to understand.
Assume that two devices from two different subdomains of a network are communicating with each other and there is an IDS instance in each subdomain. The traffic of such communication will be analyzed by both IDS unnecessarily. Besides, there are other scenarios that an IDS can be overloaded with analyzing a vast amount of traffic, while other IDSs still have the unutilized capability.

Goals of the Thesis

You, as a well-prepared researcher are in charge of creating a platform that can monitor the workload of IDS instances in an SDN network and redirect the traffic load toward them accordingly. As the first milestone of your journey, you should develop a virtual network consist of the common network elements and control its connectivity based on SDN technology. As the next steps, you will place multiple IDSs in appropriate locations and monitor their activity. Following, you will develop an algorithm that can assign traffic to IDSs to analyze or engineer the traffic path dynamically according to the workload of IDSs in the network. In the end, you will finish your journey by defencing your thesis and introduce yourself to the academic community with (a) valuable publication(s). Besides, you will have an open source platform to maintain that protect online activity of many people.

Keywords

SDN, IDS, Load Balancing, Network Security

Contact:
Hossein Doroud: <h.doroud@tu-berlin.de>

Website:
www.tkn.tu-berlin.de