Security Services as Software Defined Network APIs

Hamid Farhadi
The University of Tokyo
farhadi@nakao-lab.org

Akihiro Nakao
The University of Tokyo
nakao@iii.u-tokyo.ac.jp

***Abstract*—Software Defined Networks(SDN) are nowadays increasingly becoming more popular. In this position paper, we discuss several applications of security services as in-network processing elements in Network Virtualization and SDNs.**

I. Introduction

In an SDN, some software, organize and manage the packet handling in the network. Moreover, they may provide some high level services for different purposes such as security. As an example, OpenFlow API allows the control plane to use some rules containing a pattern that matches on bits in the packet header that can be followed by some actions. While similar works, as an API, can help providing network operators with routing, load balancing and access control, still there is a huge gap to fulfill SDN goals.

II. In-network Security Services

In this section, we briefly introduce examples of in-network processing applications that can be exposed as building blocks of SDNs to the user.

- *Intrusion Detection*: Intrusion Detections Systems are widely deployed to protect networks. In large networks usually alerts from many sensors are gathered in Security Operation Center (SOC) to be correlated and analyzed. In a sliced environment a virtual SOC (vSOC) as a service will reduce user costs significantly. The slice environment provider entity can provide an already deployed and configured vSOC and assign an instance of the vSOC service to a specific slice. Therefore, only the traffic of that specific slice goes to the vSOC and process through different components of Security Information and Event Management (SIEM) system. The vSOC may have some GUI which shows report graphs and charts related to the slice owner.
  Moreover, a Honey-slice is another interesting security service in sliced environments. A Honey-slice is a honeynet that is deployed in virtualized environment to evade hackers, it can be in a similar topology of the user slice with similar background traffic. This mapping and the level of information exposed to the honey-slice can be configurable. In the worst case, the Honey-slice can be a copy of the user slice with the same configuration.
- *Malware Detection*: One of the important steps in malware analysis is monitoring the behavior of malwares in the network. To do so, we need and isolated environment that logs all behaviors of the malware. A malware analysis slice that simulates a real network can be a useful tool. The slice is a completely isolated environment that monitors and records malware activities from outside of the slice.
  Another useful example is Network-based File Carving, where as a Deep Packet Inspection (DPI) activity, the SDN, looks for Portable Executables(PE) crossing the network and automatically scans them for known viruses. An alternative is to scan PEs using sensitive Dynamic Heuristic methods to provide Virology Labs with unknown threats and suspicious PEs.
  Additionally, Antivirus as a service within the network would be beneficial for some other services such as email servers which deal with files. Instead of having a separate antivirus locally on different server machines it can be provided as an in-network service. They can also act as on-demand scanning tools for clients within the networks.
- *Computer Forensics*: gathering network evidences is a useful tool for forensics. The community proposed some methods for payload attribution and similar light logging approaches in order to document the traffic in a storage friendly manner. An in-network service for specific network slices that need this level of security is an attractive feature for users. With the growth of fast and small storage systems that can be embedded as the first level storage inside the network controls, providing such services is achievable.

III. Conclusion and Future Direction

In this position paper, we present some possible services in building blocks of SDNs. In-network processing services as Application Programming Interfaces can be used as an aid for SDN programmers. Currently, most of the efforts toward SDN development is focused on control plane. In this paper, we tried to extend this view to data plane centric applications. Although, control plane programmability of network controls provides some flexibility, it can not reach the deepness of the flexibility of data plane programmability where we can measure, decide and act directly based on the data in application layer. We hope this can be directive approach for the community to carry on the research towards highly flexible, deeply programmable and fast Software Defined Networks.