An Architecture for Intrusion Prevention using Software Defined Networks

Antonio Gonzalez Pastana Lobato, Ulisses da Rocha Figueiredo, Otto Carlos M. B. Duarte
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

***Abstract*—Security is a challenge in future networks. Future Internet proposals rely on virtualization to provide multiple types of networks sharing the same physical infrastructure. This proposal takes advantage of the programmability offered by Software Defined Networks (SDN) to provide an architecture for an Intrusion Prevention System. We developed and tested a prototype in FITS (Future Internet Testbed with Security), a platform for experimenting Next-Generation Internet proposals.**

I. Introduction

Intrusion Prevention is one of the main challenges of Internet security today. Most of Internet's security is hosted on the network's edge. However, the majority of attacks occurs internally. In this scenario, not only a Intrusion Detection Systems, but also a Prevention System, which takes actions in order to block the attack, is required.

Future Network is based on the pluralist approach, by allowing distincts logical networks in the same physical substract. In order to obtain this level of abstraction, the virtualization paradigm is introduced. In a virtualized environment resources, such as memory, CPU and bandwidth, are shared between multiple virtual machines. In this context, network virtualization is achieved, through the usage of virtual machines as network elements.

The architecture proposed in this paper provides an Intrusion Prevention System for future networks based in Software Defined Networks's flexibility. SDN's plane separation provides more programmability to control the virtual switches, and therefore, creates a managing environment for an Intrusion Preventing System.

II. Intrusion Detection Operation Modes

There are two modes [1] in which Intrusion Detection works in the network:

On-path Detection: The IDS is placed on the packets route, so that every packet goes in the IDS to be analyzed and then forwarded to it's destination. This method prevents that any malicious packet in this path goes unseen. However, as every packet must be analyzed before being forwarded, the IDS works as a packet buffer, affecting the network's performance.

Off-path Detection: In this approach the IDS is a separate node of the network connected to a switch, and every packet that arrives in this switch is mirrored to the port in which the IDS is connected. This way, although its possible that some packets of a threat goes to it's destination before it's classified as a malicious flow, the network performance is not affected.

Since in the proposed architecture, one of the main goals is Quality of Service (QoS), the Off-path Detection is adopted.

III. Software Defined Network

Software Defined Network is based on the plane separation paradigm, the data plane and the control plane. The data plane is responsible for forwarding the traffic, while the control plane act as the network intelligence, defining where will be the packet's next hop.

OpenFlow [2] is a protocol for SDN that relies on the plane separation paradigm. This protocol defines 12 fields to match a packet header, which is used by the control plane to install a flow table entry in the data plane. In the OpenFlow protocol, only the first packet of each flow is forwarded to the controller, who install the flow rule in the switch for the rest of the packets.

IV. Implementation and Architecture

In order to implement our proposal, the FITS [3] was used. The Future Internet Testbed with Security provides a virtual network environment for experimentation of new applications for the Internet.

In our architecture, the controller is configured to install the rule to send the packet both to it's destination and to the Intrusion Detection System. Whenever the Intrusion Detection System identifies a malicious flow it generates an alarm that is sent to the controller. When the controller is notified by the IDS, it lists all the flows installed in the OpenFlow switches and set a drop action to all the flows that matches the malicious one. That way, the malicious flow is blocked near it's origin.

V. Conclusion and Future Work

Software Defined Network can be a useful tool for an Intrusion Prevention System, due to it's capability to both mirror the network traffic and block the malicious flow as soon as the Intrusion Detection System notifies the controller.

For future work, a study on the scalability of our proposal is intended, allowing multiple IDS virtual machines running in the same network.

Acknowledgments

This work was supported by FINEP, FUNTTEL, CNPq, CAPES, and FAPERJ.

References

[1] J. R. Ballard, I. Rae, and A. Akella, "Extensible and scalable network monitoring using opensafe," *Proc. INM/WREN*, 2010.

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: in campus networksenabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, 2008.

[3] P. H. V. Guimaraes, L. H. G. Ferraz, J. V. Torres, I. D. Alvarenga, C. S. Rodrigues, and O. C. M. Duarte, "Experimenting content-centric networks in the future internet testbed environment," in *Workshop on Cloud Convergence, ICC*, 2013.