15. Ilmenauer TK-Manager Workshop
Technische Universität Ilmenau, 17. Mai 2019
DOI: 10.22032/dbt.38489
URN: urn:nbn:de:gbv:ilm1-2019200270

Protection of SDN Networks Against the Existing Security Threats

by M.Sc. Abdullah Alshra'a

Abdullah Soliman Alshra'a machte seinen Bachelorabschluss und erlangte den akademischen Grad Master of Informatics an der al Albayt University in Jordanien. Seit Februar 2017 ist er Promotionsstudent im Fachgebiet Kommunikationsnetze der TU Ilmenau. Seine fachlichen Interessen liegen im Bereich Schutz der SDN-Netzwerke vor bestehenden Sicherheitsbedrohungen.

DOI: 10.22032/dbt.38499

Motivation

Software-defined networking (SDN) is a physical separation of the network control plane from the forwarding plan, where a control plane controls several devices. SDN is a new architecture that is manageable, cost- effective, adaptable, dynamic, and suitable for a high bandwidth to enable today's applications to perform well.

The SDN Security has been a major attention for its deployment. SDN threats are more sophisticated to defend since control messages issued by a compromised controller look legitimate [1]. The researchers are doing a good effort to deals with the injection packets or Daniel of Serves attack from illegal users. the switch sends any new event or request to the controller which is responsible for computing a suitable path and supplies the switches with new rules. The attackers exploit this procedure to inject the network by packets which come to increase the overhead or trying to hack the network. The authors add methods to the controller to check every single packet. However, the methods do not prevent the forged packet from entering the controller, thus more overhead and it is possible to disrupt the controller [3] [2].

In general, our research aims to uncover a new security vulnerability in the OpenFlow communication process, topology management service and Rest API in the SDN controller. It presents a novel attack against the SDN controller and demonstrates the feasibility of such attack. Moreover, the PhD work discuses several possible solutions to mitigate security vulnerabilities.

Approach

The dependence on the target controller to deal with bad packets is sufficient to give these packets a good chance to get in the controller, thus increasing the overhead or even inserting malicious instructions to steal or disrupt the target information. Our proposal, the INSPECTOR is a hardware device added to the SDN architecture to protect a compromised controller from a packet injection attack by verifying the authentication of Packet-In Messages accessing network resources [1]. Figure 1 shows such topology which uses the inspector.

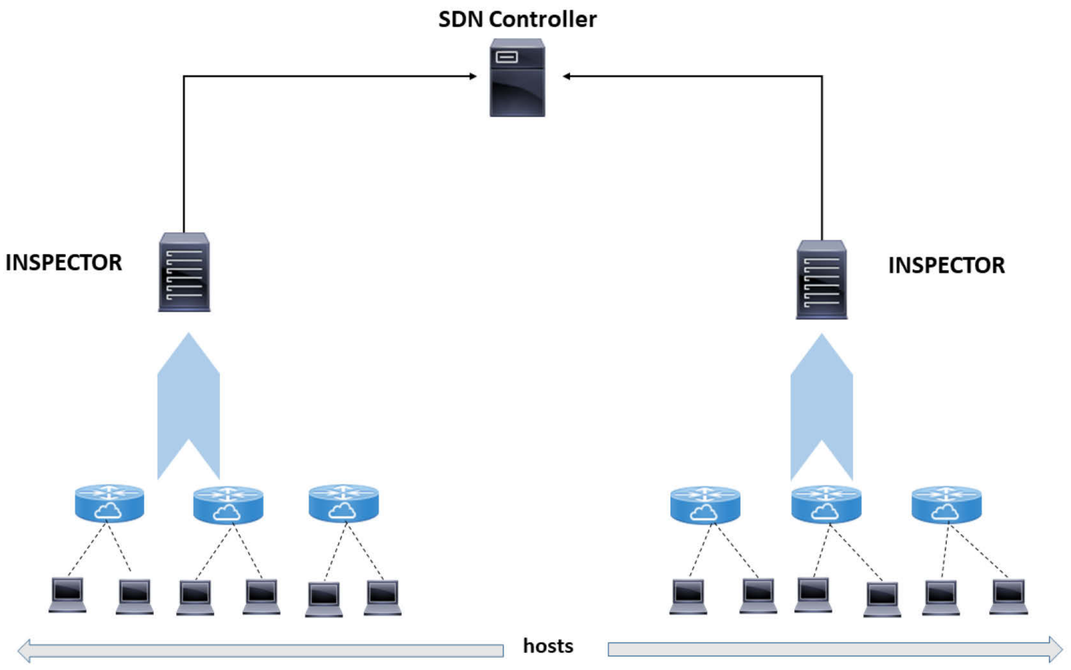

Figure 1: Inspector Location between the switches and the controller

Simulation

To investigate the feasibility and the effect of our work, we compared INSPECTOR to the PacketChecker module [2] which was assumed to deal with a flow of packets with the same share of forged addresses (e.g. 1000 packets). With simulations, we show that this INSPECTOR device efficiently stops the attack and enhances the controller performance under malicious attack. In our experiment, every single packet has a different address. To do that, the implementation is tested using the Mininet emulator where the Ryu controller 1.3 is used to manage a Fat Tree topology with a server [1].

Conclusion and Future Work

In our simulations, we prove that using an additional hardware device to deal with the forged packet is an efficient approach and significantly enhances the controller performance during the attack. As a future work, the next step is to add a trusted third party ensuring the INSPECTOR would not be compromised. Furthermore, the search method could be reduced to a constant time by using a smarter data structure.

References

[1] Alshra'a AS, Seitz J. Using INSPECTOR Device to Stop Packet Injection Attack in SDN. IEEE Communications Letters. 2019 Feb 4.

[2] Deng, Shuhua, et al. "Packet Injection Attack and Its Defense in Software-Defined Networks." IEEE Transactions on Information Forensics and Security 13.3 (2018): 695-705.

[3] Deng S, Gao X, Lu Z, Li Z, Gao X. DoS vulnerabilities and mitigation strategies in software-defined networks. Journal of Network and Computer Applications. 2019 Jan 1; 125:209-19.