Poster: Denial-of-Service Attack Using Host Location Hijacking in Software-Defined Networks

Yumin Sim
Department of Information Security
Seoul Women's University
Seoul 01797 Republic of Korea
Email: soyouhe773@naver.com

Hae Young Lee
Department of Information Security
Seoul Women's University
Seoul 01797 Republic of Korea
Email: haelee@swu.ac.kr

***Abstract*—This paper presents a data-to-control plane saturation based denial-of-service (DoS) attack in a software-defined network. In the proposed DoS attack, an attacker impersonates a number of hosts by exploiting the security flaws of the host tracking service (HTS). As HTS could misrecognize such fake migrations of the hosts, the flow tables associated with the hosts may need to be totally reconstructed, so that parts of the network may be slowed down or even unavailable due to data-to-control plane saturation. The feasibility of the proposed attack is shown with experimental results.**

I. Introduction

Software-defined networking (SDN), which decouples the centralized control system (the control plane) from the underlying systems (the data plane), has recently emerged as a promising technology for future networks. Meanwhile, researchers have also investigated security issues in SDN. For example, an attacker can launch *data-to-control plane saturation based denial-of-service (DoS) attacks* by injecting a large number of anomalous packets [1]; the centralized controller would receive a large number of *Packet-In* messages asking about rules for handling the packets, and thus could be overloaded. Also, by exploiting security weaknesses in the host tracking service (HTS), an attacker can launch *host location hijacking attacks* [2], in which he/she attempts to hijack the traffic towards a host by impersonating the host.

In this paper, we propose another type of data-to-control plane saturation based DoS attack in an SDN network, by hijacking the locations of multiple hosts. In the proposed DoS attack, an attacker attempts to impersonate a number of host, to make HTS misrecognize mass migrations of the host, which could lead to mass updates of the flow table associated with the hosts, possibly throughout the entire network. Thus, the controller could be overloaded, so that parts of the network may be slowed down or even unavailable. The impact of the proposed DoS attack, in terms of network performance, is shown with preliminary experimental results.

II. Host Location Hijacking Based DoS Attack

In an SDN/OpenFlow network, locations of all hosts can be tracked with the host tracking service (HTS). This can be achieved by monitoring *Packet-In* messages that the controller has received from the switches. For instance, if a host has migrated to another location and sent a packet from that location, HTS can recognize such a migration by receiving a *Packet-In* message that encapsulates the packet. The flow tables associated with the host would be also reconfigured for providing seamless service. However, HTS may not support host authentication mechanisms [2]. Thus, an attacker could easily impersonate a target host, which could make HTS misrecognize the location of the host. That is, he/she could hijack the traffic towards the host.

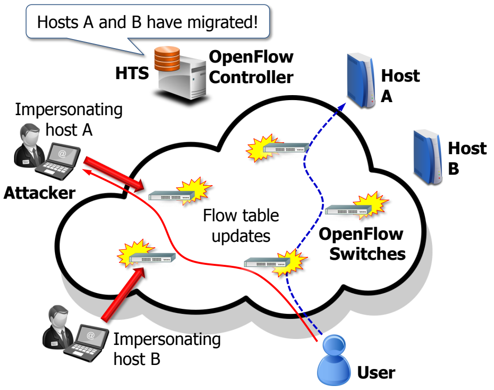

Fig. 1. Host location hijacking based DoS attack.

In the proposed DoS attack shown in Fig. 1, the host location hijacking attacks are used to consume the resource of the controller (i.e., data-to-control plane saturation). An attacker's goal is to make parts of the network slowed down or even unavailable by consuming the controller's resource. To this end, he/she attempts to impersonate a number of (preferably well-known) hosts so that HTS could misrecognize mass migrations of the hosts. To provide seamless service, the flow tables associated with them would need to be totally reconfigurated, possibly throughout the entire network, which may result in data-to-control plane saturation. Thus, parts of the network may be slowed down or even unavailable. Even if the tables are not updated immediately according to the network's policy, they would be eventually updated as benign users visit the hosts. If the hosts impersonated by the attacker are well-known enough to be very frequently visited by the users, this could also lead to data-to-control plane saturation, resulting in service denial.

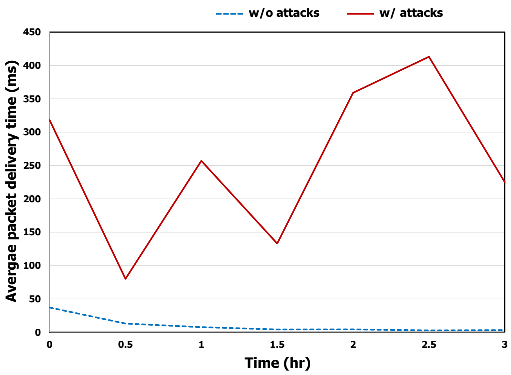

Fig. 2. Performance impact of the proposed DoS attack.

The proposed attack differs from the existing ones. Shin's DoS attack [1] mainly targets a few switches, while the proposed attack might affect the entire network (if an attacker could impersonate a very large number of hosts). Although Hong's DoS attack [2] also uses *topology poisoning*, which includes host location hijacking and link fabrication, service denial could be achieved by killing ports in his attack.

III. Preliminary Evaluation

We have performed feasibility experiments to show the performance impact of the proposed DoS attack. An SDN was emulated by Mininet, in which Open vSwitch products handled packets under the control of a Floodlight controller. Fig. 2 shows the average delivery time of ICMP packets in the network. As shown in the figure, the proposed attack impacted heavily on the performance of the network. We are also expecting that the impact of the attack would increase with the complexity of the network.

IV. Conclusion and Future Work

This paper presented a data-to-control plane saturation based DoS attack in an SDN network, in which mass updates of the flow tables due to fake host migrations are used to achieve data-to-control plane saturation. The proposed attack may affect the performance of the entire network. The preliminary experimental results were given to show the performance impact of the attack.

As future work, we will observe the effect of the proposed attack under the existence of some countermeasures against DoS attacks (e.g., FloodGuard [3]) or topology poisoning attacks (e.g., TopoGuard [2]). Based on the observation, we will study its variations as well as countermeasures. Also, we will try to use link fabrication [2] to conduct another type of DoS attacks.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (NRF-2013R1A1A1006542).

References

[1] S. Shin and G. Gu, "Attacking softare-defined networks: A first feasilbity study," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*. ACM, August 2013, pp. 165–166.

[2] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning network visibility in software-defined networks: New attacks and countermeasures," in *Proceedings of the 2015 Network and Distributed System Security*. Internet Society, February 2015, pp. 1–15.

[3] H. Wang, L. Xu, and G. Gu, "Floodguard: A dos attack prevention extension in software-defined networks," in *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, June 2015, pp. 239–250.