SDN Forensics - A Review

Samriddha Sinha

BE Undergraduate Student, CSIS department, Birla Institute of Technology and Science, Pilani, Rajasthan, India

November 16, 2021

1 Introduction

SDN architecture has not yet been researched enough from a security perspective. Hence, SDNs are more vulnerable to attacks than traditional network systems. The main objective of the paper is to throw light on SDN forensics, an area which has not received enough attention. It details the problems, evidence collection points, and further challenges faced by SDN forensics.

2 Why SDN Forensics

Software-defined networking separates the control plane from the data plane. While it simplifies the network structure, it leads to an increased risk of attack. Each of the SDN layers (application, control and infrastructure) can provide evidence against malicious activity on the network. However, the authenticity of the evidence must be ensured in order to reliably determine the cause and nature of the attack.

SDN forensics is simpler than traditional network (TN) forensics. The structured nature of SDNs and the separation of the different layers aid in forensic investigation. For TNs we usually need to investigate at the packet level, but in SDNs a higher level search can yield valuable evidence.

3 Evidence Collection

Layer division enables easy identification of locations in a particular layer where evidence may be found

3.1 Application Layer

At this layer, application logs are the most useful. These can be retrieved in the OpenDaylight (ODL) controller by using the Open Services Gateway initiative (OSGi) architecture.

3.2 Control Layer

Host tracking service (HTS) and link discovery service (LDS) are the two main tools in this layer. HTS keeps track of all hosts using the network, hence identifying malicious users. Nevertheless, it may be "poisoned", when HTS sends wrong information about the network, allowing a bad actor to hijack the network.

LDS controls the various links between the switches. It is possible that a bad actor might insert fake links into the LDS, allowing them control. It can be prevented by using the metadata sent through the packets and alarming the network administrator whenever a fake link is detected.

3.3 Infrastructure Layer

The rules in the flow table of an OpenFlow (OF) switch can help trace back malicious activity. The counter for various attributes of a switch provide helpful evidence. On the basis of such evidence, the network traffic may be redirected towards specialised middleboxes that analze various attacks.

3.4 Northbound and Southbound Interfaces

At this layer API logs can provide evidence. REST API is used in the northbound interfaces. Since it uses URI strings, it can help find out the commands the attacker was trying out on the network. API logs can be examined without interrupting the network.

4 Steps in SDN Forensics

The different stages in an SDN forensic investigation are:

- Identification of evidence collection points based on the type of attack.
- Collection of evidence, ensuring privacy and integrity of the collected evidence.
- Analysis of the collected evidence using dedicated servers, middleboxes or third-party software.
- Reporting the findings as future reference against such attacks.

5 Challenges

5.1 Trustable Log Data

Logs are vital to SDN forensics, hence data integrity in the logs is vital for successfully identified the cause of the attack. Till now no standard approach has been devised to protect the logs from manipulation.

5.2 SDN Performance Enhancement

SDN forensics consumes network time and computation power. Hence during an investigation the network may experience slowdown if the controllers are not able to handle the load.

5.3 Synchronization of Evidence

The log data across multiples geographies and time zones must be synchronized in order to present the true picture of the attack mechanism.

5.4 Source Identification

A traceback mechanism must be provided in order to find the real source of the attack. Few solutions have been proposed, but they are not practical yet.

5.5 Middlebox Security

The middleboxes trusted with testing the attack must themselves be secure. Complete dependence on middleboxes is prone to risk as they themselves may be compromised

6 Conclusion

Through the paper we examined the need for SDN forensics, the process and potential pitfalls. More research needs to be made in this field in order to secure SDNs against attacks, as they are becoming increasingly vital in maintaining our large-scale networks.