Forensic investigations in SDN networks

Authors:

Izzat Alsmadi

Department of Computer Science, University of New Haven

Samer Khamaiseh

Department of Computer Science, Boise State university

Introduction

- SDN is a recent networking architecture that can be classified under *programmable networks, where users and their applications can have more control on how to manage their network traffic*.

- SDN has two significant characters :
  - It separates control from data. SDN switches include only data.
  - Control in SDN is aggregated for all network switches remotely in a software-based controller.

Introduction

- OpenFlow is a protocol that is defined to allow SDN switches to communicate with their controller.

- OpenFlow makes switching and routing protocols open rather than proprietary or vendor specific (i.e. in classical switches).

Research Problem

- SDN provides the opportunity to interact with the network and its traffic in real time.
- Having a tool that performs forensic analysis of SDN network will help in revealing and the diagnoses possible security vulnerabilities.
- Ultimately, we like to see autonomous SDN-based forensic tools that can:
  - Monitor in real time all in/out network traffic without significantly impacting normal traffic.
  - Detect any possible ***abnormal behavior***
  - Take actions to mitigate such ***abnormal behavior*** to ensure that network normal activities are not compromised.

Forensics' Knowledge Extraction

- We developed a forensic analysis tool that performs forensic analysis.
- We consider our work as "preliminary" toward extracting knowledge relative to the process of forensic analysis.
- We used input files (i.e. network PCAP file and switch memory dump) as the two inputs to extract knowledge about the network and its traffic.

Forensics' Knowledge Extraction

- Extracted files are arranged based on our knowledge of OpenFlow protocol and what can be defined as "relevant" to network forensics.

- In their current forms, our files can assist in the investigation process and direct investigators on where to focus (as an alternative to look through large dump and PCAP files).

Examples of Extracted Information

- Special Protocols:
  - ARP, ICMP and other protocols can trigger some security concerns.
  - Network attacks such as DoS, flooding, spoofing, etc. can all be triggered based on looking at traffic of such protocols.

Examples of Extracted Information

- Packet Header Types:
  - Tool can evaluate each packet header type (TCP, IPv4) in it is own context.
  - For example, whether the packet is of TCP or UDP, IPv4 or IPv6 will cause the trigger of different roles for forensic investigations and possible network attacks, vulnerabilities, etc.
- For example, in TCP/UDP packet headers, certain flags can be checked if they are true or false where they can be flags for certain attack types (e.g. SYN,SYN/ACK, etc.)

Examples of Extracted Information

- Source, Destination IP and MAC Addresses:
  - Tool generates files that's help us to know each packet or certain sequence of sender and receiver packets (layer 2 and layer 3 information).
- Ports:
  - Tracking information about incoming our outgoing packet ports. In/Out port numbers can be relevant to many attacks or forensic investigations.
  - Switch and controller in OpenFlow communicate through known specific ports.
  - known applications are known to be using certain ports.
  - Rules can be made to alert in case of any packet request beyond the range of known ports.

OF switches and Forensic-Related Information

- The tool also can perform forensic analysis on switch memory dump files.

- Following are examples of Forensic-related information that can be extracted from switch memory dumps [Given the knowledge of OpenFlow protocol]:

- OpenFlow Protocol Messages and actions:
  - Certain keywords such as (ofp header,OFPT, OFPAT) can be used to indicate OpenFlow Protocol messages between controller and switches. Tracking those messages is very important.

OF switches and Forensic-Related Information

- OVS ofctl and OVS vsctl:
  - Those most of the flow-related commands (e.g. addFlow, dumpFlow, etc.).
  - Can by very significant form the security perspectives.

- OpenVSwitch :
  - OpenVSwitch includes another class of important commands related to the virtual switch.

Conclusion

- We developed an SDN-based forensic tool to provide efficient and readable information to SDN forensic or network analysts.

- During the implementation process we consider to balance between the following factors:
  - The amount of information to provide or extract from network activities.
  - The relevancy or usefulness of information to any possible security analysis.
  - The generalization of information to be usable in other scenarios or types of SDN network outputs.

QUESTIONS

- Contact Information:
  - Samerkhamaiseh@u.boisestate.edu
  - alsmadi@gmail.com
- Tool Source Code in GitHub:
  - https://github.com/alsmadi/SDN-Competition