Demo Title:

Experimentation of SDN-Supported Collaborative DDoS Attack Detection and Containment

Tommy Chin, Xenia Mountrouidou, Xiangyang Li, Kaiqi Xiong

One-sentence layman's description:

This demo shows a collaborative monitoring and correlation approach to mitigate the effects of the surge in network traffic of a flooding Denial of Service attack that can cause loss of service for legitimate sites.

Who should see this demo?

Attendees interested in Cybersecurity attack detection, and mitigation techniques.

Demo description paragraph(s):

"Elevator speech" description that identifies (a) what you are demonstrating and (b) why it is important. This description may be used for advance publicity and to help attendees identify the demonstrations they wish to see.

Software-defined networking (SDN) and OpenFlow offer great support to dynamically adapt a network and to access data on different network layers as needed. Such advantages have been driving recent research efforts to develop new security applications and services. However, most studies on attack detection and containment have not really differentiated their solutions from the traditional ones, without fully taking advantage of the unique capabilities provided by SDN. Moreover, even if some of these studies provide interesting visions of what can be achieved, they stop short of presenting realistic application scenarios and experimental results. We present a novel attack detection and containment approach that is coordinated by distributed network monitors and controllers/correlators centralized on an SDN OpenFlow Virtual Switch (OVS). With different views and information availability, these elements collaboratively detect signature constituents of an attack that possess different characteristics of scale and detail. Therefore, this approach is able to not only quickly issue an alert against potential threats followed by careful verification for high accuracy, but also balance the workload on the OVS.

We apply the proposed approach to TCP SYN flood attacks using Global Environment for Network Innovations (GENI). This realistic experimentation has provided us with insightful findings helpful to our goal toward a systematic methodology of SDN-supported attack detection and containment. First, we have demonstrated through experimentation the scalability of our collaborative scheme. Second, we have studied how the combination of alerts by the monitor and deep packet inspection by the correlator, can increase the speed and accuracy of attack identification. Our experiments, in the context of a small to medium corporate network, have demonstrated the effectiveness and scalability of the SDN-supported detection and containment approach..

List of equipment that will need AC connections (e.g. laptop, switch, monitor):

Laptop and a monitor.

Total number of wired network connections (sum standard IP and VLAN connections):

One wired network connection.

Number of wired layer 2 VLANs (if any):

One VLAN for single network connection

Specify VLAN number, if known, approximate bandwidth, and whether tagged or untagged.

Any number (including VLAN 1)

Number of wireless network connections (include required bandwidth if significant):

N/A

Number of static addresses needed (if any):
N/A

Monitor (y/n, specify VGA or DVI):
VGA Monitor with minimal of resolution of 1440x900 or 1280x1024

Number of posters (max size poster boards are 30" x 40"):
One

Special requests:
Include any specific network connectivity needs
(e.g. VLANs to a particular GENI location, projects you'd like to be near, etc.)