SAND2019-8172D

The Center for Cyber Defenders

Expanding computer security knowledge

CosmicDust: Virtualized Cluster Security

Julian Tuminaro, Carnegie Melon University; Jonathan Grimes, Texas A&M University;
Andrew Chu, Purdue University

David Burton 5832; Rick Strong 5832; Tim Toole 5831

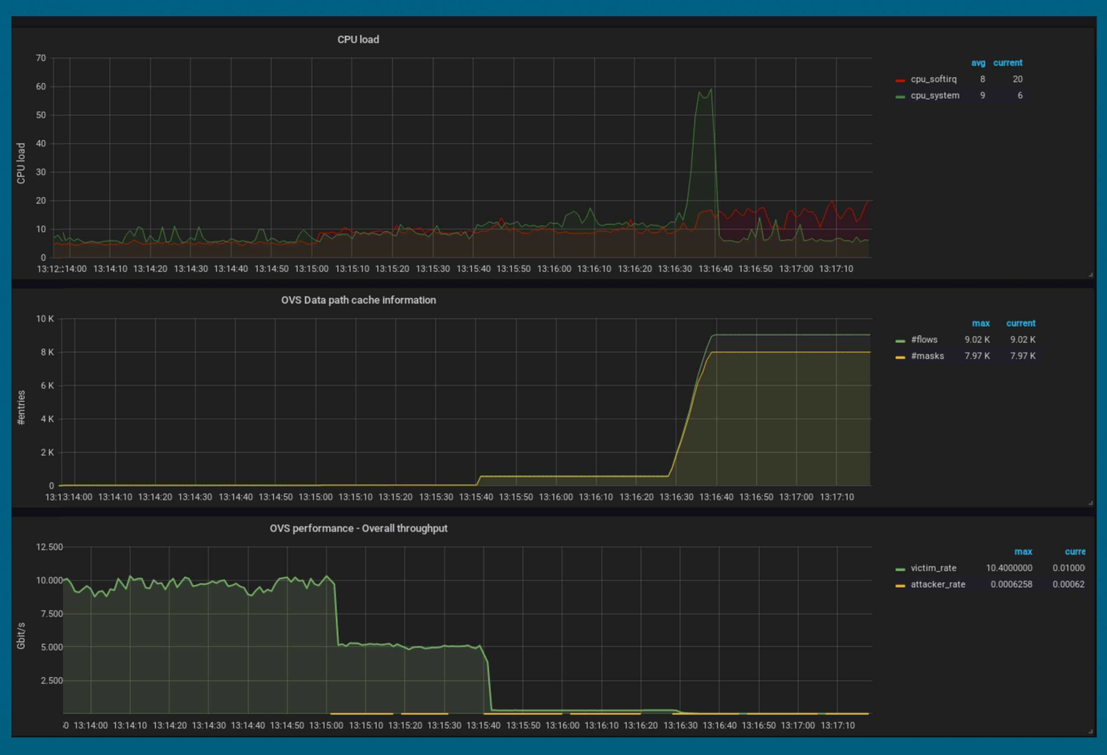
Problem Statement:

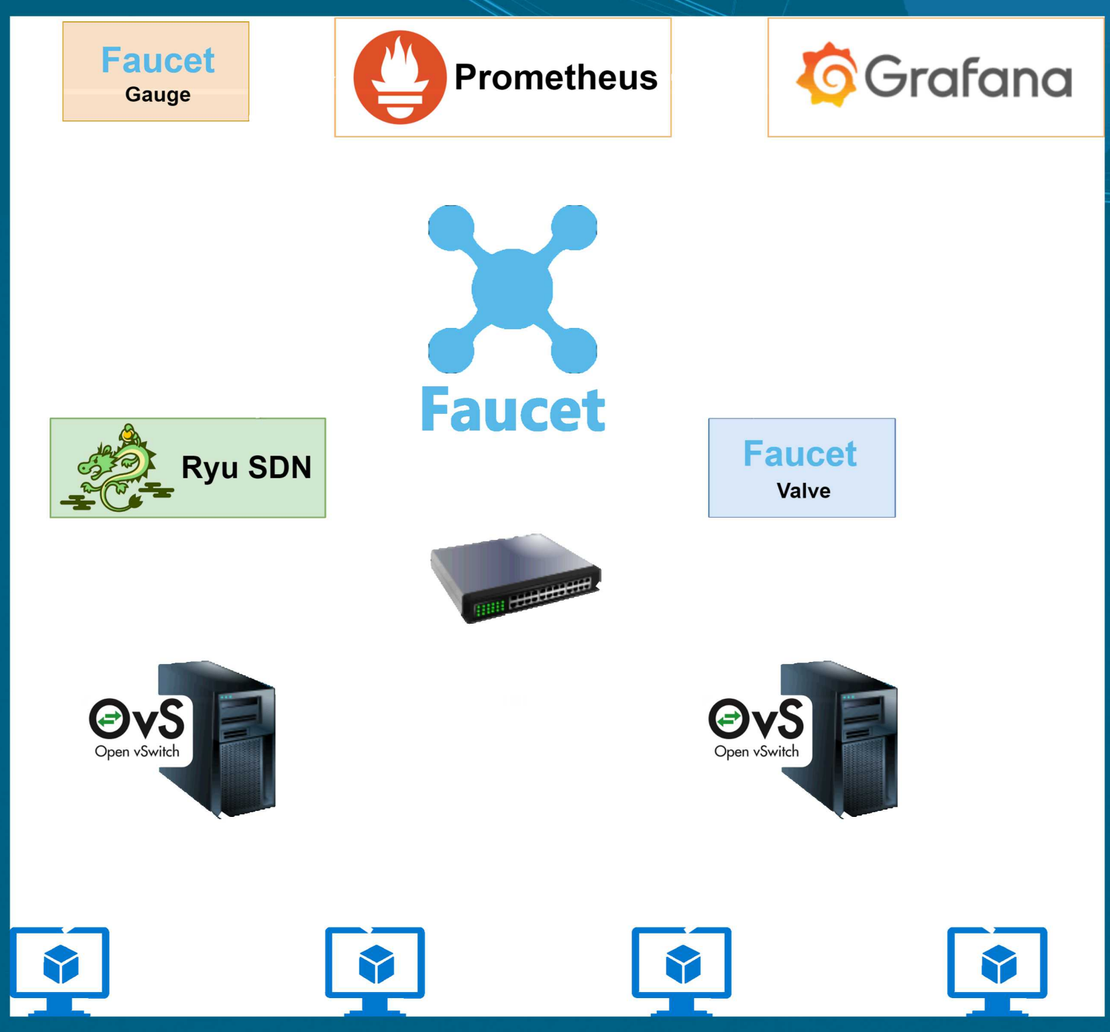
The Open vSwitch (OVS) is a virtual switch designed to provide a comprehensive environment for the OpenFlow communication protocol. Fast with high programmability and generality, OVS has become the leading backend for OpenStack deployments. As this configuration has become more widespread, it becomes increasingly important that stable and secure performance is maintained.

The *megaflow cache* which runs in kernel space performs arbitrary bitwise wildcarding on its entries in order to achieve the level of efficiency OVS is known for. However, certain flow rules and traffic patterns can exhaust the flow caching architecture and force OVS to default to the *ovs-vswitchd* daemon (running in the user space). This transition between the kernel space and user space has significant consequences for performance.

Impact and Benefits:

- Increase awareness of the risks associated with using the megaflow cache
- Showcase security usage of virtualized SDN
- Boost resiliency of deployed SDN clustered environment





Cluster Configuration

Objectives and Approach:

- Build physical and virtual clusters of nodes, virtual machines, and containers
- Develop a virtualized environment enabling connectivity through all modules (OVS, Faucet)
- Generate realistic traffic for the created virtual environment and simulate the megaflow cache vulnerability
- Visualize impact and effect of various flow rules and traffic patterns through use of Grafana and Prometheus
- Establish a concise attack and defense model

Results:

- Instantiate virtualized *Software Defined Network* (SDN) cluster
- Visualize impact of implemented traffic patterns throughout cluster
- Create a highly replicable application of the megaflow cache vulnerability
- Obtain conclusive indicators of the megaflow cache vulnerability

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration