Project: Securing networks with P4

Organisation	University of Amsterdam
Deliverable	Report

Identifying the path followed by malicious traffic is needed to secure networks. The knowledge of the ingress and egress points, as well as the intermediate hops, allows in principle to counteract the attacks.

The challenge is that identifying such paths requires proper and accurate monitoring; this means in turn to choose a sampling rate that allows to determine the path across the various devices, while not making the reporting burden too heavy for the networking devices. These limitations were clearly outlighted in previous work we did with the CoreFlow framework, which we tested in the ESnet network. There we observed that the NetFlow sampling rate was limiting our ability to identify and correlate flows to security incidents.

Understanding and evaluating these trade-offs is therefore an essential element in assessing how strongly we can secure a network. To quantify them we turn to P4.

P4 programs provide us with an innovative way to identify and store flow information as well as give us insight on the shortcomings of other collection tools. Concretely we intend to investigate how to use P4 to identify and store the first packet of every flow passing through in the network alongside information over the path taken. A mechanism to so this would be to use suitable Bloom filters that are invoked during the action moment of P4 programs.

If this proves to be possible and reliable, an outcome of this research would a clear way to assess of how changing the number of flows we can detect affects performance of response.
The new CORSA switches present in the SURFnet testbest support the new extended version of the P4 language and we will use them for our experimentation.