

# P4CONTROL

---

## Motivation

- Traditional network security protection methods can not identify cross-host attacks, and the malicious traffic issued by the stepping board cannot be correctly identified.
- Common protection methods are usually based on traffic characteristics matching, lack of fine-grained management and control of information flow.
- Traditional protection relies on a central control plane, which leads to performance bottlenecks in high-traffic network environments.

## Innovation

- P4CONTROL innovatively extends DIFC to the network layer, and controls the transmission of information flow by directly executing DIFC policies in the network data plane. It enables fine-grained information flow control.
- P4CONTROL is real-time, dynamic, administrators can dynamically modify the policy, so as to achieve a rapid response to attacks.
- P4CONTROL is closer to the idea of a zero-trust architecture, where the flow of information is managed according to strict access control policies, even inside the network.

## Structure

- P4CONTROL uses programmable switches to handle traffic, which ensure that information is transmitted according to rules by label matching.
- DIFC tags are used to mark the information and permissions of data streams, so as to manage sensitive data.
- In a reasonable marking process, for each passing traffic, the device needs to be marked with the traffic. On the one hand, it is used to manage permissions, and on the other hand, it can be used to trace sensitive data.
- NETCL is used to facilitate the administrator to customize the management policy.

## Discussions

- P4CONTROL requires additional hardware and configuration, and it is difficult to be compatible with older devices.
- P4CONTROL is difficult to support dynamically changing topologies and cannot be plug-and-play for new devices, requiring additional configuration by the administrator.

## Thoughts

- In my view, the biggest highlight of P4CONTROL is that it extends DIFC from operating system level to network level, realizes fine control of information flow through programmable switches and eBPF technology, and can manage and protect cross-host traffic in real time. This design greatly improves the real-time and efficiency of the system.

- To me, P4CONTROL seems to be more in the traditional direction of what I think of as cybersecurity. However, I only have a partial understanding of this direction, and it will be difficult to get started. If I participate, I will need to read some papers in advance to learn relevant knowledge.