Securing P4-SDN Data Plane against Flow Table Modification Attack

Kshira Sagar Sahoo, Monowar Bhuyan

Dept. of Computing Science, Umeå University, Sweden.

{Ksahoo,monowar}@cs.umu.se

Abstract: Security in Software Defined Network (SDN) architecture is becoming the most substantial challenge. This paper introduces a novel threat model focused on flow table modification in the P4-programmable SDN data plane, outlining an attacker's stochastic manipulation of flow rules from a compromised switch. A detection framework is proposed to identify the malicious switch within the network by utilizing the thrift port. Moreover, a fuzzy-rule-based mitigation strategy has been proposed to identify the severity of attacks. The feasibility and effectiveness of the methodology are evaluated using a developed testbed setup by employing Facebook datacenter fabric topology in a Mininet emulator and BMv2 switch.

Index Terms—SDN, Flow table security, Flow rule modification, attack, P4 switch, Data plane