Vulnerabilities in SDN Due to Separation of Data and Control Planes

Volume 179 - Number 31

Year of Publication: 2018

Authors:
S. Faizullah, S. AlMutairi

Abstract

Tremendous advancements over the past several decades revolutionized the networking research and technological industry, however, it is still dominated and remains hardware based. Such legacy networks are inflexible, hard and costly to scale and manage. Software defined networking (SDN) is a new approach to networking which enable comprehensive network programmability. SDN architecture bifurcates the data and control plane thereby simplifies network management. In this new architecture, the control plane consists of networking intelligence and the policy making ability is moved to a centralized entity called as controller. Commonly, SDN uses OpenFlow as the communication interface between the data and control planes. This separation while providing great opportunities for scalability, also introduces new vulnerabilities. We identify certain scenarios for vulnerabilities in the OpenFlow semantics that can subject the controller to distributed denial of service (DDoS) attack which is unique to SDN due to the new architecture where the control plane is separated from the data plane. We also explore some reactive mechanisms that can detect and help to devise techniques to prevent impending DDoS attack on an SDN controller.
References

7. A. Doria, J. Hadi Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal, and J. Halpern, “Forwarding and control element separation” (ForCES) protocol specification, RFC 5810 (Proposed Standard), March 2010,

Index Terms

Computer Science Networks

Keywords

Software Defined Networking; SDN; SDN Vulnerabilities; DDoS; Cloud Computing; OpenFlow.