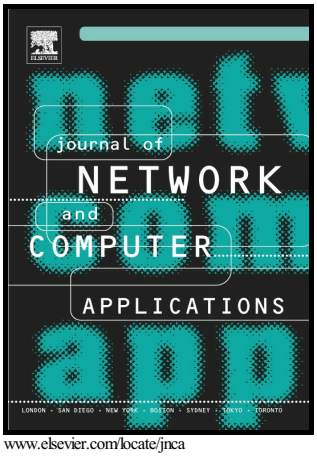
Identifying Cyber-Attacks on Software Defined Networks: An Inference-based Intrusion Detection Approach

Ahmed AlEroud, Izzat Alsmadi



www.elsevier.com/locate/jnca

PII: S1084-8045(16)30344-7
DOI: http://dx.doi.org/10.1016/j.jnca.2016.12.024
Reference: YJNCA1807

To appear in: *Journal of Network and Computer Applications*

Received date: 1 July 2016
Revised date: 8 November 2016
Accepted date: 15 December 2016

Cite this article as: Ahmed AlEroud and Izzat Alsmadi, Identifying Cyber-Attacks on Software Defined Networks: An Inference-based Intrusion Detection Approach, *Journal of Network and Computer Applications*, http://dx.doi.org/10.1016/j.jnca.2016.12.024

Identifying Cyber-Attacks on Software Defined Networks: An Inference-based Intrusion Detection Approach

Ahmed AlEroud[a], Izzat Alsmadi[b]

[a]Yarmouk University, Jordan
[b]University of Texas A&M, San Antonio, USA
Ahmed.aleroud@yu.edu.jo
ialsmadi@tamusa.edu

Abstract—

Software Defined Networking is an emerging architecture which focuses on the role of software to manage computer networks. Software Defined Networks (SDNs) introduce several mechanisms to detect specific types of attacks such as Denial of Service (DoS). Nevertheless, they are vulnerable to similar attacks that occur in traditional networks, such as the attacks that target control and data plane. Several techniques are proposed to handle the security vulnerabilities in SDNs. However, it is fairly challenging to create attack signatures, scenarios, or even intrusion detection rules that are applicable to dynamic environments such SDNs. This paper introduces a new approach to identify attacks on SDNs that uses: 1) similarity with existing attacks that target traditional networks, 2) an inference mechanism to avoid false positives and negatives during the prediction process, and 3) a packet aggregation technique which aims at creating attack signatures and use them to predict attacks on SDNs. We validated our approach on two datasets and showed that it yields promising results.

Keywords: ***Software defined networks; Information security; Intrusion detection; Graph mining, Denial of service attacks; Security architecture.***

I. INTRODUCTION

In network security, autonomous network agents learn their network topology and the nature of threats in their network to write or update their roles with the least amount of human effort. There are many learning and evolutionary activities that the complete network agent may require. The amount of automation in those activities depends on the complexity of the design of those agents, their network, goals, etc. The recent evolution in programmable networks such as Software Defined Networks (SDNs) opens the possibility to extend the automated activities to ultimately build network agents that are fully autonomous in the network.

Despite the opportunities and benefits of SDNs, practitioners and researchers argue that SDNs are vulnerable and easier to target [1, 2, 3]. When the logic of the forwarding behavior is centralized and allocated in the controller, a single point of failure and attack is created. Both exploiting the vulnerabilities in the controller or the communication links between the switch and controller can lead to several attacks such Denial of Service (DoS) [4] and Host Location Hijacking Attacks [5]. Man in the Middle (MIM) is yet another potential attack in which the adversary may break the link between the controller and its switches, then claim the control of such connection [5]. To summarize, there are possible attack scenarios that make the current architecture of SDN non-secure, which requires more attention to various security aspects of SDNs.

Yet, there are several challenges when creating security techniques to mitigate such attacks on SDNs. First, there is a need to create sophisticated security measures which do more than just discarding or forwarding flows. Specifically, statistical and signature matching techniques need to be combined with the flow rule production. In particular there is a need to "implement complex quarantine procedures of the flow producer, or they could migrate a malicious connection into a counter-intelligence application in a manner not easily perceived by the flow participants"[5]. Second, the existing procedures which are used to create security applications depend on the architecture of the controllers used to manage the network. The implications of the current controller architectures are equally problematic for implementing security mediation services. In particular, the element responsible for security mediation should operate independently from those elements it mediates [5]. As such, there is a need to create platform independent security applications for SDNs. Third, since handling traffic in SDNs is quite dynamic, it becomes difficult to discover different types of attacks using anomaly detection techniques since they will lead to high percentage of false positives. Finally, there is an increasing number of Zero-day attacks and SDNs are not protected against such attacks. There have been some attempts to create anomaly detection techniques that discover Zero-day attacks