A Hybrid Approach to Security Attack Detection in Containerized Applications

Yuhang Lin
ylin34@ncsu.edu
North Carolina State University
Raleigh, North Carolina

Xiaohui Gu
xgu@ncsu.edu
North Carolina State University
Raleigh, North Carolina

ABSTRACT

Security attack detection aims for low false positive rate and high true positive rate. Existing approaches often have a trade off between false positive rate and true positive rate. We present a hybrid approach to security attack detection in containerized applications with the goal of significantly reducing the false positive rate while maintaining a high true positive rate. Our initial experiments show hybrid approach can reduce false positive rate by 51.4% while only reduce true positive rate by 6.3%.

CCS CONCEPTS

• **Security and privacy → Virtualization and security**.

KEYWORDS

Container Security, Anomaly Detection, Machine Learning

1 INTRODUCTION

Recent studies show containers are vulnerable to security attacks [1, 5]. Thus a lot of researchers have come up with different approaches to protecting containers including analyzing container images [2], dynamic attack detection with on demand patching [6] and a defend system for privilege escalation [3].

In our previous work [4], we propose a classified distributed learning framework (CDL) to achieve efficient security attack detection for containerized applications. We conduct a case study of false positives. Figure 1 shows that there are a large number of false positives whose reconstruction errors are within the range of [100%, 110%] of our reconstruction error threshold for detecting attacks. We define those data points with reconstruction errors within the range of [100%, 110%] of threshold as the boundary cases. If we can handle those boundary cases in a more intelligent way, we can achieve much lower false positive rate with little impact on the detection rate.

In this work, we present a new hybrid approach to security attack detection in containerized applications with the goal of significantly reducing the false positive rate while maintaining a high true positive rate. Our approach combines unsupervised application learning and supervised attack learning to achieve the goal. Every time when we meet a boundary case, we get the prediction probability and predicted label from the supervised learning model. If the most probable prediction is normal or if the maximum prediction probability is below a certain threshold, we believe the current data sample is a false positive.

We evaluate our approach using data collected from 33 real world attacks in recent years. Our results show this hybrid approach can detect 33 out of 33 attacks with false positive rate of 0.53%. Compared with the original version of CDL, it can reduce false positive rate significantly by 51.4% while only reduce true positive rate by 6.3%.

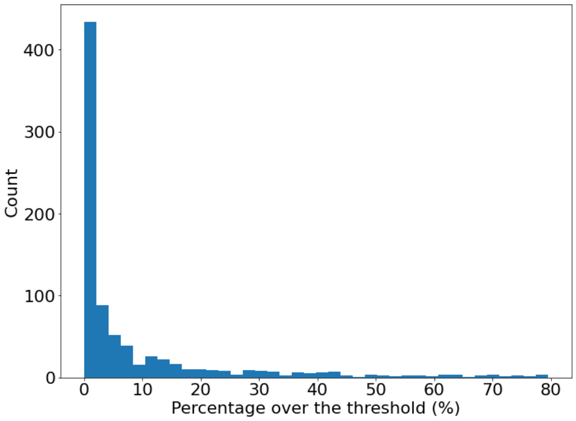

Figure 1: Percentage of the autoencoder reconstruction errors of false positives over the threshold of 99 percentile training reconstruction error.

REFERENCES

[1] 2017. Docker image vulnerability research. https://www.federacy.com/docker_image_vulnerabilities

[2] Soonhong Kwon and Jong-Hyouk Lee. 2020. DIVDS: Docker Image Vulnerability Diagnostic System. *IEEE Access* 8 (2020), 42666–42673.

[3] Xin Lin, Lingguang Lei, Yuewu Wang, Jiwu Jing, Kun Sun, and Quan Zhou. 2018. A measurement study on linux container security: Attacks and countermeasures. In *Proceedings of the 34th Annual Computer Security Applications Conference*. 418–429.

[4] Yuhang Lin, Olufogorehan Tunde-Onadele, and Xiaohui Gu. 2020. CDL: Classified Distributed Learning for Detecting Security Attacks in Containerized Applications. In *Annual Computer Security Applications Conference (ACSAC '20)*. Association for Computing Machinery, 179–188.

[5] Rui Shu, Xiaohui Gu, and William Enck. 2017. A study of security vulnerabilities on Docker hub. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*. 269–280.

[6] Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, and Xiaohui Gu. 2020. Self-Patch: Beyond Patch Tuesday for Containerized Applications. In *2020 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS)*. IEEE, 21–27.