健康資訊交換系統中之容器安全
The Container Security in Healthcare Data Exchange System

國立中山大學資訊工程學系
Department of Computer Science and Engineering
National Sun-Yet-San University, Taiwan

110 學年度大學部專題製作競賽
Bachelor’s degree graduation project in 2021

Member: Chih-Hsuan Yang (B073070047)
Advisor: Chun-I Fan

October 10, 2021

Abstract

This research proposes a mechanism to enforce the system call a specific policy in the container, which is deployed in runtime. This policy is designed for the FHIR healthcare data exchange standard's container, which could guarantee the FHIR server does not have unsupported behavior and takes almost zero overhead. Recently, many companies use containers to run their microservices since containers could make their hardware resources be used efficiently. And the newest healthcare data exchange standard FHIR (Fast Healthcare Interoperability Resources) [1] has been implemented in a container by IBM, Microsoft, and firebase. The deployment of FHIR in a container is a trend in the digital world [2] . However, containers are not sandboxes [3] . Containers are just isolated processes. Therefore, if hackers or malicious software could sneak into the container that would be a new cyber attacking surface in nearly future.

Contents

Chapter 1

Introduction

1.1 Container and Linux Kernel

1.2 FHIR

1.2.1 RESTful API and Data Structure

1.2.2 Why IBM FHIR server

1.3 Data and Privacy

Chapter 2

Related Works

2.1 Collecting System Calls

2.2 Find-granted Permission Control

2.3 Recently Exploited Vulnerabilities

2.3.1 Five Stage of Malware

2.4 Virtual Environment Performance Benchmark

Chapter 3

Preliminary

3.1 Container's Components

3.1.1 Namespaces

3.1.2 Cgroups

3.1.3 Seccomp

3.2 Programs in Execution

3.2.1 The task_struct in Kernel

3.2.2 Capabilities

3.3 User Mode Linux

3.3.1 Sandbox Security

3.3.2 gVisor

3.4 The (e)BPF

Chapter 4

Proposed scheme

4.1 Workflow

4.1.1 Scan Base Image

4.1.2 Signing

4.1.3 Check Image and Policy

4.1.4 Enforce Policy

4.2 Rolling Updates

Chapter 5

Analysis

5.1 Attacking Surface

5.2 Time Consuming

5.3 Statistics

Chapter 6

Benchmark

6.1 Latency

6.2 Thruputs

Chapter 7

Conclusion

7.1 Better Architecture

7.2 Future Machine Learning in Kernel

Bibliography

[1] HL7. *FHIR homepage*. URL: https://www.hl7.org/fhir/.

[2] A. Ahmed and G. Pierre. “Docker Container Deployment in Fog Computing Infrastructures”. In: *2018 IEEE International Conference on Edge Computing (EDGE)*. 2018, pp. 1–8. DOI: 10.1109/EDGE.2018.00008.

[3] Ian Goldberg et al. “A Secure Environment for Untrusted Helper Applications Confining the Wily Hacker”. In: *Proceedings of the 6th Conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6*. SSYM’96. San Jose, California: USENIX Association, 1996, p. 1.