Symbolic Modeling of Micro Services for Intrusion Detection

William Blair
Boston University

Frederico Araujo, Teryl Taylor, Jiyong Jang
IBM Research

Overview

- Micro Services split monolithic applications into individual services that run across computing clusters.
- An immutable container image defines each container within a micro service.
- An image consists of a layered filesystem that holds the OS environment, an application, and any dependencies.
- We perform symbolic modeling over images in order to automatically derive stateful security policies.
- These policies express the side effects benign workloads would issue and allow a cloud operator to detect intrusions from container telemetry.

Related Work

Intrusion Detection

Methods

- Consider a Program $P$, Input $x$, and Trace $T = \text{Eval}(P, x)$
- Let $\tau$ represent either network traffic or system calls made by $P$
- Use the following approaches to detect anomalies in $P$

Reference Monitoring
Define Model $M$ for $P$ and check whether $M, \tau$

Automata
Define Automata $A \vdash P$ and check whether $A$ accepts $\tau$

Data Mining & Machine Learning
Define Classifier $F$, Training Data $D$, and check whether $F(D) = \text{Benign}$

Architecture

DevSecOps Behavior Analysis

EntryPoint

Security Policy $\tau$

Cloud Operator

Symbolic Modeling

Docker Image

Binary Analysis Platform

Container Telemetry

Delete Process Flows

Threat Model

SysFlow Trace $T$

Benign Case

Malicious Case

Container Reuse

Benign Case

Malicious Case

Related Work

Intrusion Detection

Methods

- Consider a Program $P$, Input $x$, and Trace $T = \text{Eval}(P, x)$
- Let $\tau$ represent either network traffic or system calls made by $P$
- Use the following approaches to detect anomalies in $P$

Reference Monitoring
Define Model $M$ for $P$ and check whether $M, \tau$

Automata
Define Automata $A \vdash P$ and check whether $A$ accepts $\tau$

Data Mining & Machine Learning
Define Classifier $F$, Training Data $D$, and check whether $F(D) = \text{Benign}$