

Symbolic Modeling of Micro Services for Intrusion Detection

William Blair
Boston University

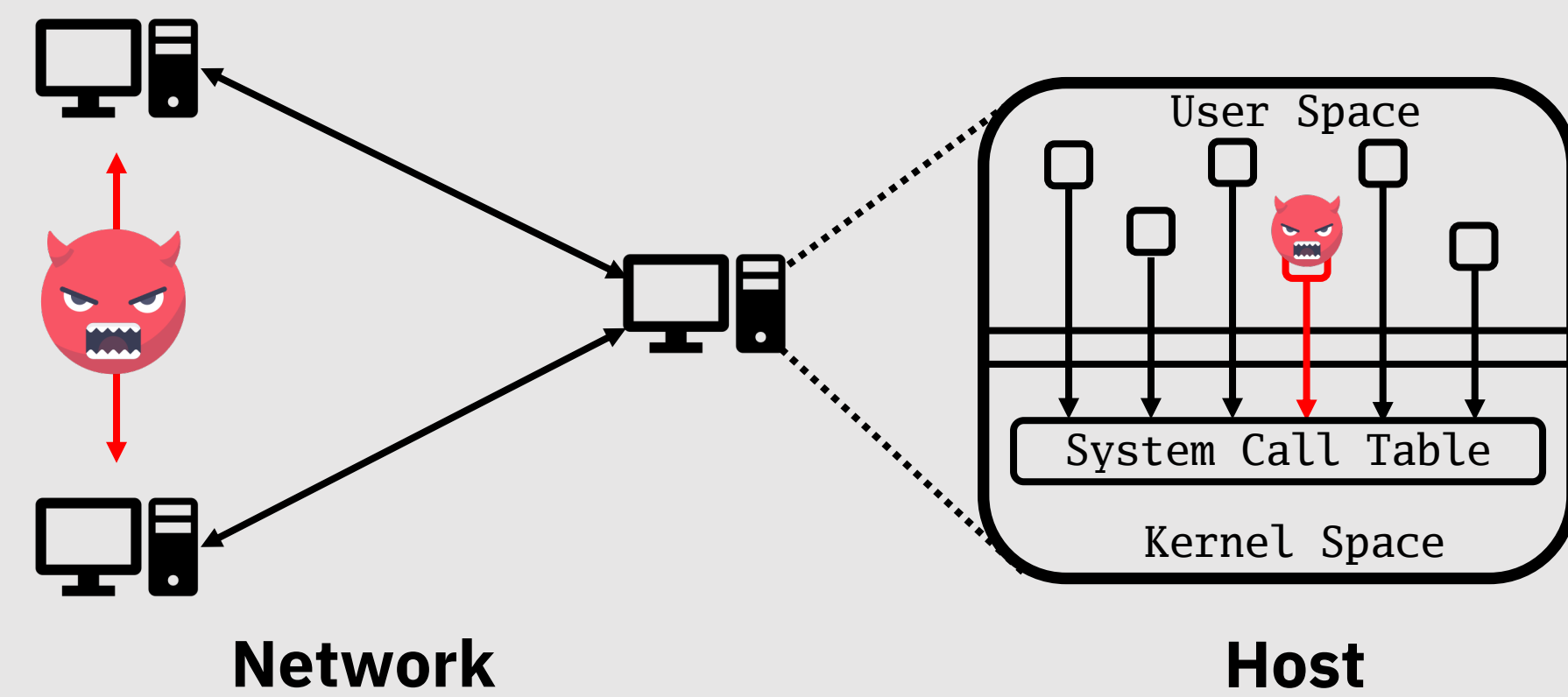
Frederico Araujo, Teryl Taylor, Jiyong Jang
IBM Research

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 $T \leftarrow Eval(P, X)$
- Let T 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 $M = T$

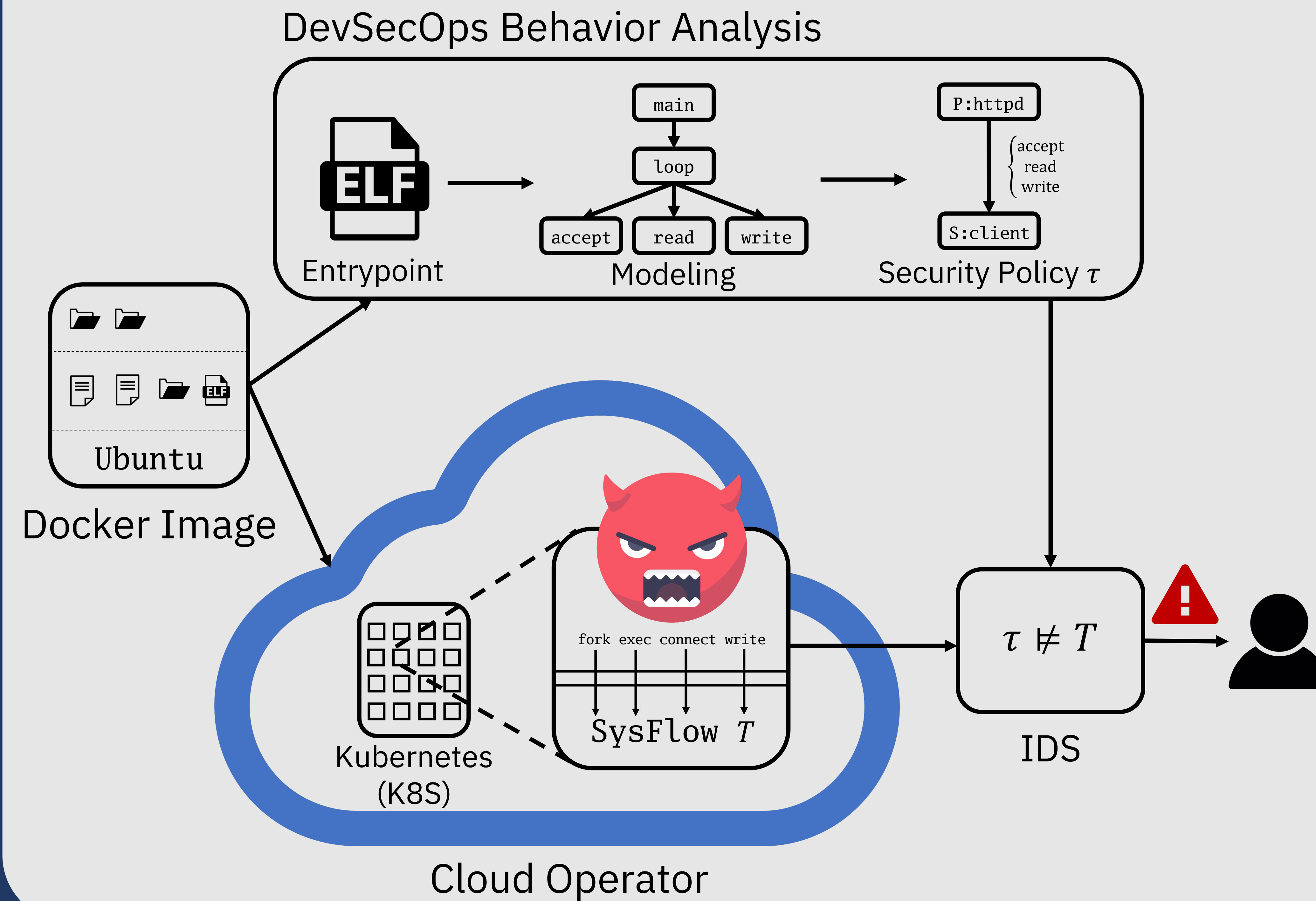
Automata

Define Automata $A \leftarrow P$ and check whether A accepts T

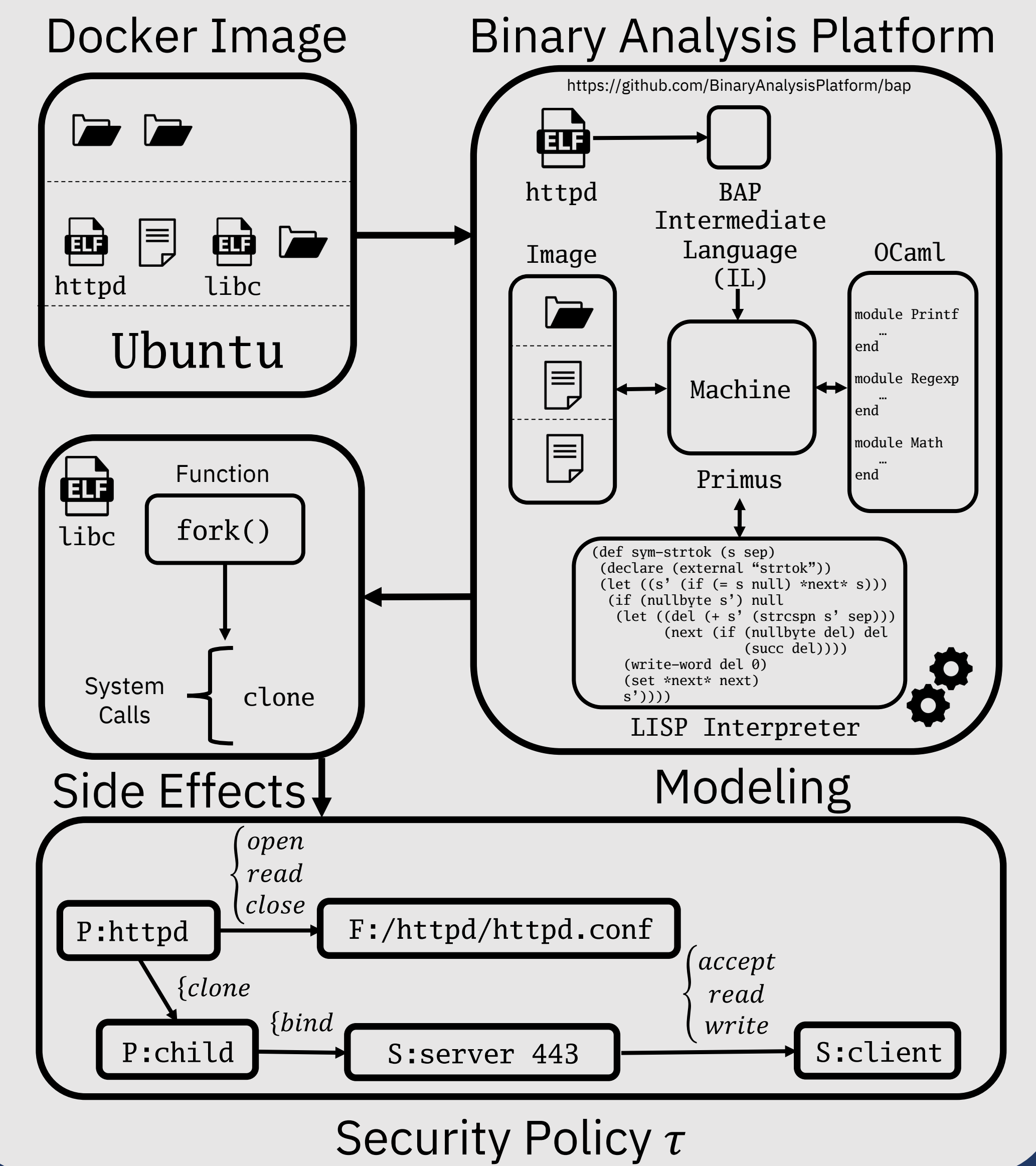
Data Mining & Machine Learning

Define Classifier F , Training Data D , and check whether $F_D(T) = Benign$

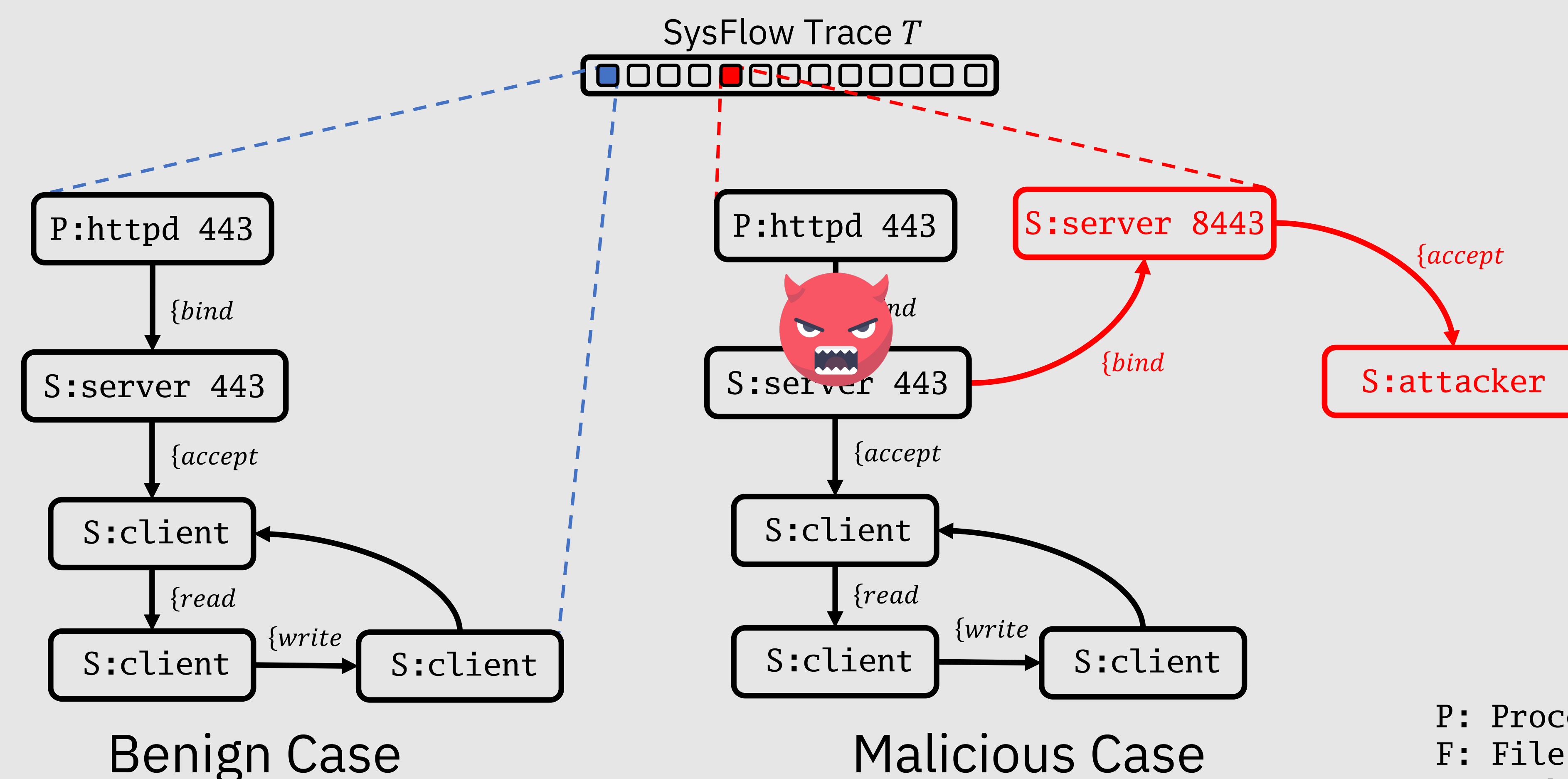
Architecture



Symbolic Modeling

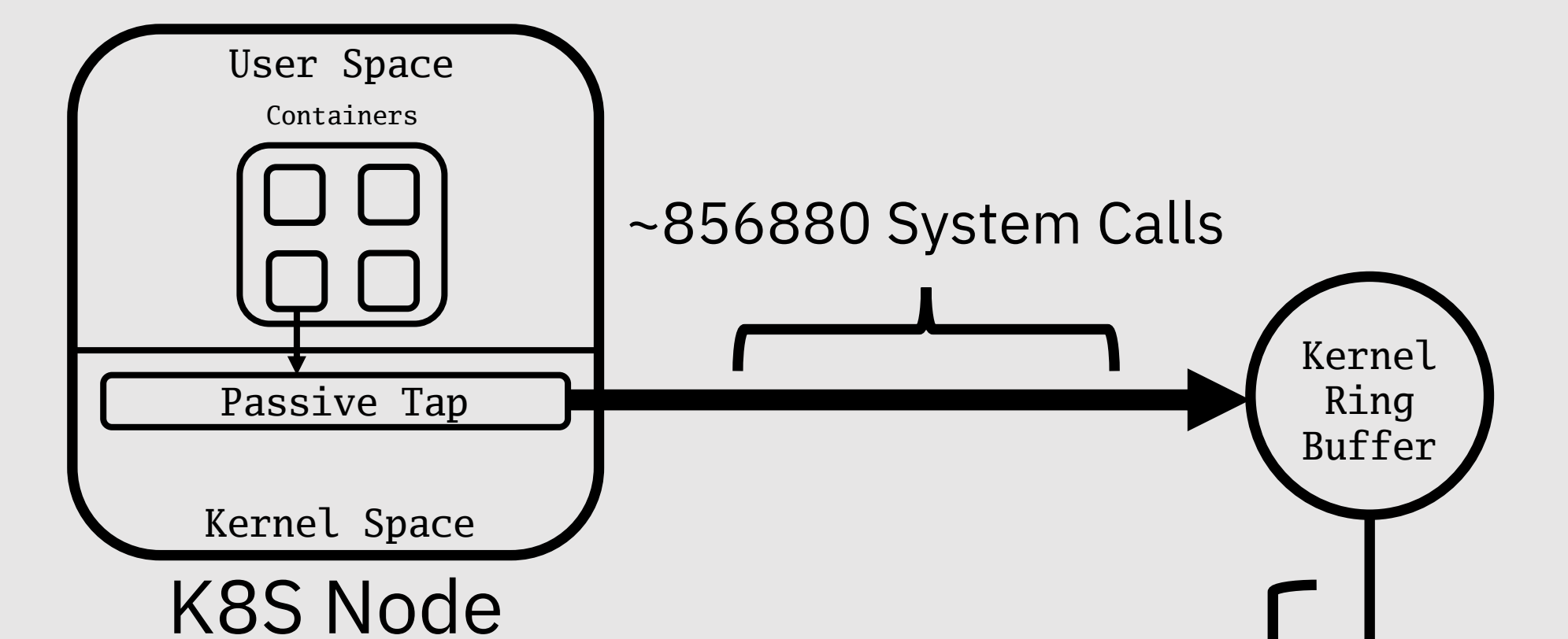


Threat Model



P: Process
F: File
S: Socket

Container Telemetry



<https://github.com/sysflow-telemetry>

| Type | Process | Events | Entity |
|------|------------|---------|-------------------|
| PE | /bin/httpd | EXEC | |
| FF | /bin/httpd | O R C | /etc/httpd.conf |
| PE | /bin/httpd | CLONE | |
| NF | /bin/httpd | A W R T | 129.42.60.189:443 |

Intrusion Detection System (IDS) Processor