The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

National Sun Yat-sen University
Advisor: Chun-I Fan

July 23, 2021

Outline

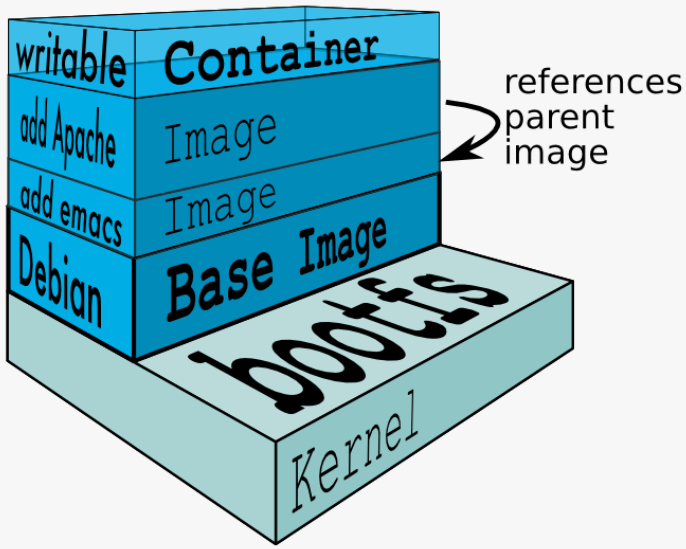
stavhaygn

Analyzing

1. LSM calling sequence of syscall
   - Quark-Engine, Bayes' theorem
   - Difficulty
     1. Hard to specify which app on witch container (context switch)
     2. Generating rules
     3. False positive is really severe
2. Check the image
   - Check the signature and hash?
   - Native docker scan supports.
   - Scan apps in layers.

```
1 FROM debian
2
3 RUN apt update -y && \
4     apt install emacs -y
5 RUN apt install apache -y
6
7 ENV HOSTNAME=Container
```

src/Dockerfile



scc@system76:/media/d/git/nsysu/cs

```
docker-image|99138c65ebc7 @ latest
├─ ca-certificates @ 20200601~deb10u1
│  └─ openssl @ 1.1.1d-0+deb10u3
│     └─ openssl/libssl1.1 @ 1.1.1d-0+deb10u3
├─ curl @ 7.64.0-4+deb10u1
│  └─ curl/libcurl4 @ 7.64.0-4+deb10u1
│     ├─ e2fsprogs/libcom-err2 @ 1.44.5-1+deb10u3
│     ├─ krb5/libgssapi-krb5-2 @ 1.17-3
│     │  ├─ e2fsprogs/libcom-err2 @ 1.44.5-1+deb10u3
│     │  ├─ krb5/libk5crypto3 @ 1.17-3
│     │  │  └─ krb5/libkrb5support0 @ 1.17-3
│     │  ├─ krb5/libkrb5-3 @ 1.17-3
│     │  │  ├─ e2fsprogs/libcom-err2 @ 1.44.5-1+deb10u3
│     │  │  ├─ krb5/libk5crypto3 @ 1.17-3
│     │  │  ├─ krb5/libkrb5support0 @ 1.17-3
│     │  │  └─ openssl/libssl1.1 @ 1.1.1d-0+deb10u3
│     │  └─ krb5/libkrb5support0 @ 1.17-3
│     ├─ libidn2/libidn2-0 @ 2.0.5-1+deb10u1
│     │  └─ libunistring/libunistring2 @ 0.9.10-1
│     ├─ krb5/libk5crypto3 @ 1.17-3
│     ├─ krb5/libkrb5-3 @ 1.17-3
│     ├─ openldap/libldap-2.4-2 @ 2.4.47+dfsg-3+deb10u2
│     │  ├─ gnutls28/libgnutls30 @ 3.6.7-4+deb10u4
│     │  │  ├─ nettle/libhogweed4 @ 3.4.1-1
│     │  │  │  └─ nettle/libnettle6 @ 3.4.1-1
│     │  │  ├─ libidn2/libidn2-0 @ 2.0.5-1+deb10u1
│     │  │  ├─ nettle/libnettle6 @ 3.4.1-1
│     │  │  ├─ p11-kit/libp11-kit0 @ 0.23.15-2
│     │  │  │  └─ libffi/libffi6 @ 3.2.1-9
│     │  │  ├─ libtasn1-6 @ 4.13-3
│     │  │  └─ libunistring/libunistring2 @ 0.9.10-1
│     │  ├─ cyrus-sasl2/libsasl2-2 @ 2.1.27+dfsg-1+deb10u1
│     │  │  └─ cyrus-sasl2/libsasl2-modules-db @ 2.1.27+dfsg-1+deb10u1
│     │  │     └─ db5.3/libdb5.3 @ 5.3.28+dfsg1-0.5
│     │  └─ openldap/libldap-common @ 2.4.47+dfsg-3+deb10u2
│     ├─ nghttp2/libnghttp2-14 @ 1.36.0-2+deb10u1
│     ├─ libpsl/libpsl5 @ 0.20.2-2
│     │  ├─ libidn2/libidn2-0 @ 2.0.5-1+deb10u1
│     │  └─ libunistring/libunistring2 @ 0.9.10-1
│     ├─ rtmpdump/librtmp1 @ 2.4+20151223.gitfa8646d.1-2
│     │  ├─ gnutls28/libgnutls30 @ 3.6.7-4+deb10u4
│     │  ├─ nettle/libhogweed4 @ 3.4.1-1
│     │  └─ nettle/libnettle6 @ 3.4.1-1
│     ├─ libssh2/libssh2-1 @ 1.8.0-2.1
│     │  └─ libgcrypt20 @ 1.8.4-5
│     └─ openssl/libssl1.1 @ 1.1.1d-0+deb10u3
├─ gnupg2/dirmngr @ 2.2.12-1+deb10u1
```

Tim

Share the kernel

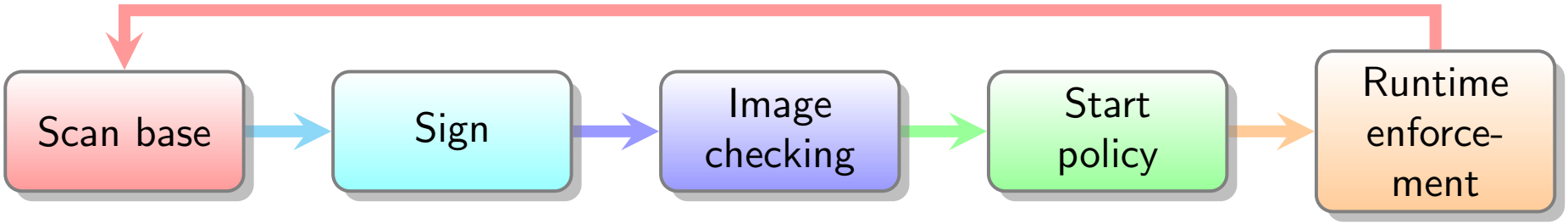
- Mixed: configuration and rule based
- built time to whitelist of syscall

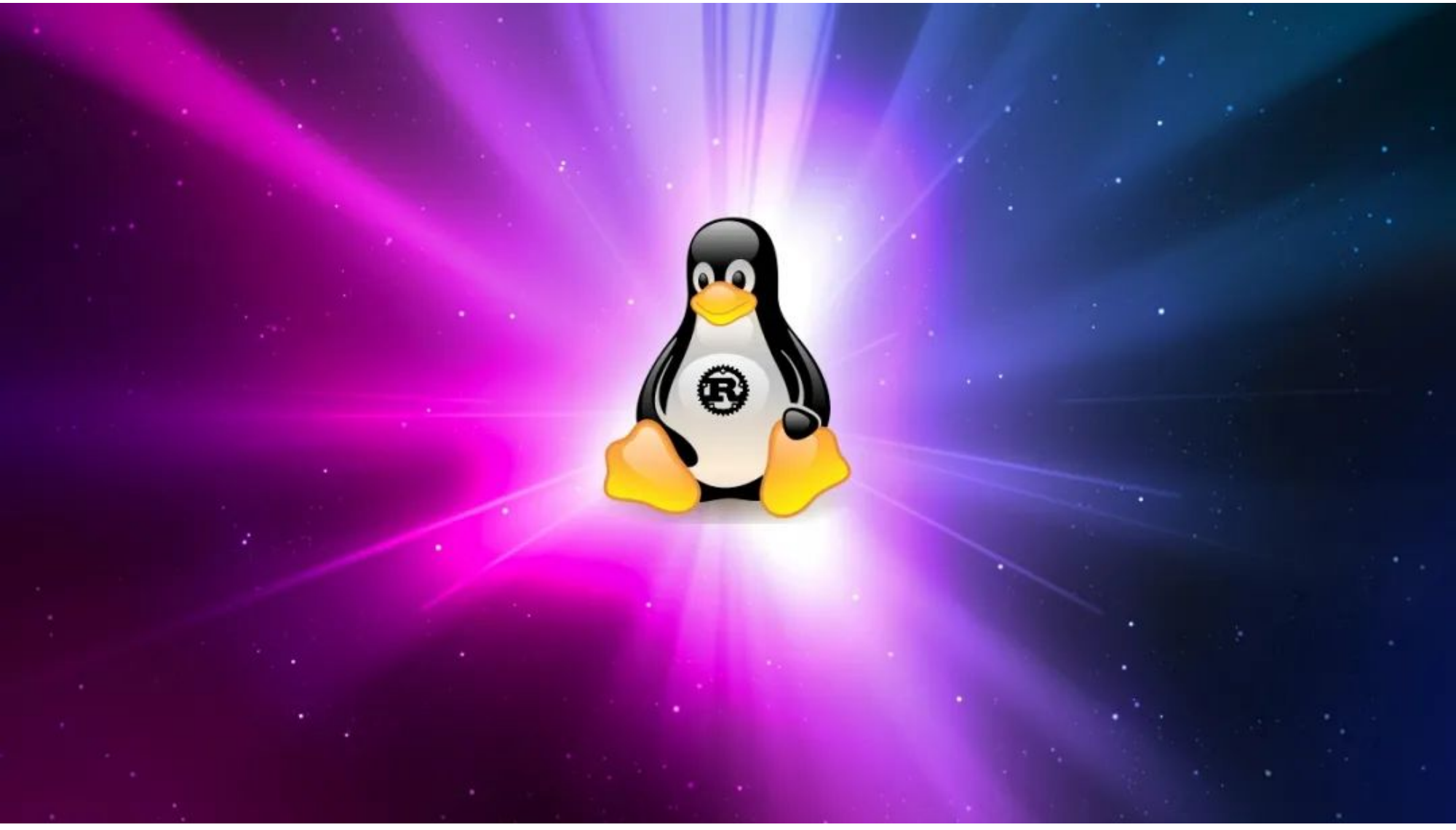
Idea and compare

- The false positive and false negative rate.
- Maybe I can mix this two mechanism together.

Compare to others mechanism?

Flow chart


Scan base
Sign
Image checking
Start policy
Runtime enforce-ment



Write kernel module in Rust