The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

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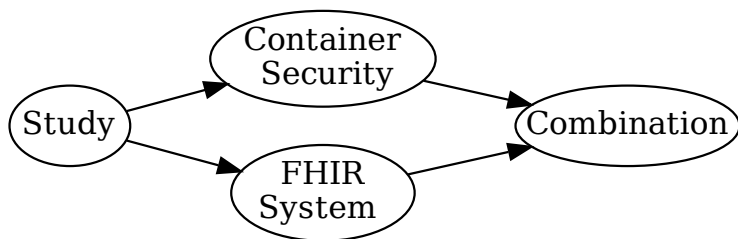Advisor: Chun-I Fan

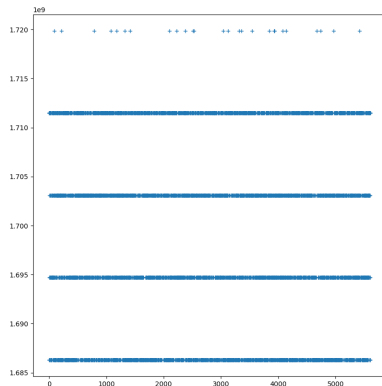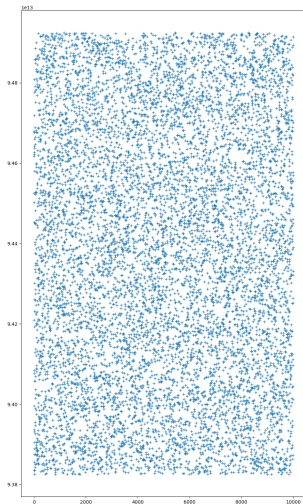April 16, 2021
v1.2

Outline

Architecture

Outcome - light weight container

Outcome - (k)ASLR

Outcome - kernel module


```
Run /init.sh as init process
  with arguments:
    /init.sh
  with environment:
    HOME=/
    TERM=linux
    hostfs=./rootfs
    mem=64M
kaslr: loading out-of-tree module taints kernel.

1694699525
random: fast init done
random: crng init done
```

```
→  0326 git:(main) ✗ less /proc/$$/maps
→  0326 git:(main) ✗ python -c 'print(1694699525)'
→  0326 git:(main) ✗ python
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import math
>>> math.log(1694699525, 2)
30.658382356126655
>>> exit()
→  0326 git:(main) ✗
```

Outcome - chroot

```
→ cont git:(main) ✗ sudo ./c ./picosh
Success on creating container
Start container: ./picosh with clone id: 2106853
In container PID: 1
$ ls
bin          dev   home  lib     mnt  picosh  root  sbin  test.sh  usr
chroot-dir   etc   jb    lib64   opt  proc    run   sys   tmp      var
$ ./jb
root@container:/# ls /media/d/git/nsysu/cs/report/presentation/0409/
images      main.bib      main.fdb_latexmk  main.nav  main.run.xml   main.tex  methFlow.pdf
main.aux    main.blg      main.fls          main.out  main.snm       main.toc  src
main.bbl    main-blx.bib  main.log          main.pdf  main.synctex.gz Makefile
root@container:/#


→ 0409 git:(main) ✗ ls
images      main.bib      main.fdb_latexmk  main.nav  main.run.xml   main.tex  methFlow.pdf
main.aux    main.blg      main.fls          main.out  main.snm       main.toc  src
main.bbl    main-blx.bib  main.log          main.pdf  main.synctex.gz Makefile
→ 0409 git:(main) ✗
```

Next steps

1. Studies
   1. Linux features
   2. Papers
2. Formal Verification
3. The Healthcare Data Exchange System part

The 3Ws

1. What this issue?
2. Why this issue?
3. How this issue?

The medical cyber security issue of the next-generation.

Why this issue

Microservice
Scalability
Manageability

Exactly microservice
Security
Performance

FAQ

1. Docker, container and virtual machine
2. FHIR? Why need container?
3. User Mode Linux
4. clone, io_uring

Q&A

Feel free to give your comments.