The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

Chih-Hsuan Yang

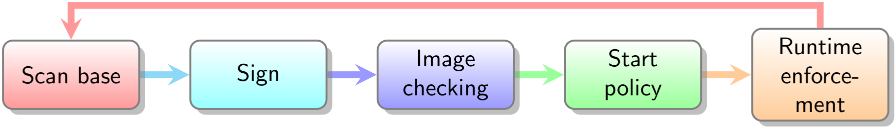
National Sun Yat-sen University
Advisor: Chun-I Fan

August 20, 2021

Outline

1. TL;DR
2. Details

Flow chart


Scan base
Sign
Image checking
Start policy
Runtime enforcement

TL;DR

Current state

- Can get system call manually.
- Can enforce the system call limitation.
- Need a registry server to register those certs.

Next state

- Generate the "sanitizer image" automatically.
- Generate the FHIR RESTful api fuzz script.
- Deploy the registry server.
- Performance benchmark.

---

1. Combine the "sanitizer image" and fuzz script.
2. Combine registry server and policy rule.

Details

Problems and solutions

Problems

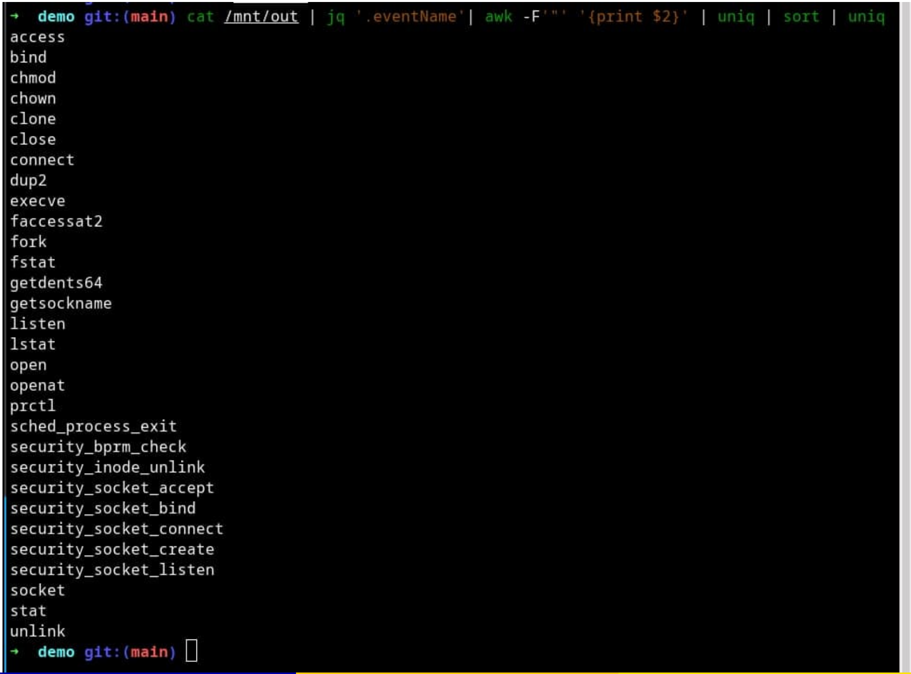
- cannot attach kprobe, probe entry may not exist
- Container/host missing library when linking
- Distro. kernel version
- Distro. library package
- Distro./Apps license

Example

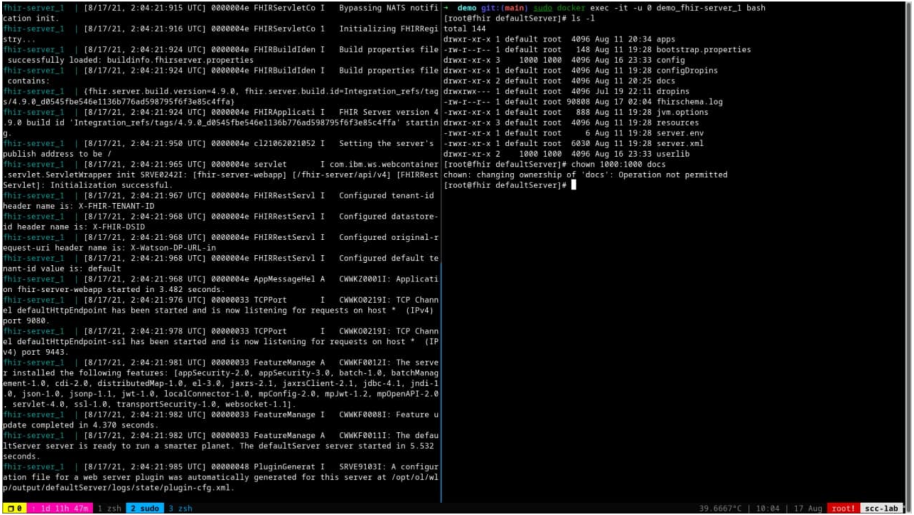
Solutions

- Change host distro.
- Change base image. (self build)
- Hack the license.

Version coherence?



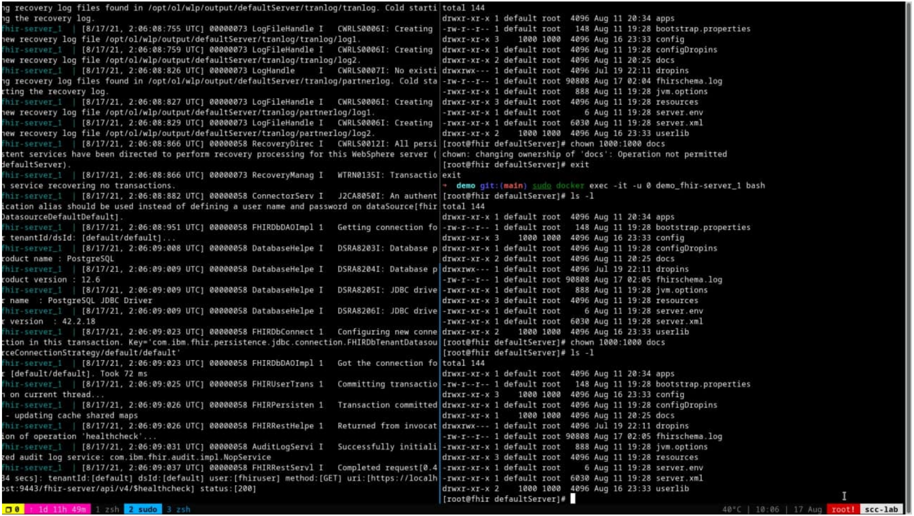
```
→ demo git:(main) cat /mnt/out | jq '.eventName'| awk -F'"' '{print $2}' | uniq | sort | uniq
access
bind
chmod
chown
clone
close
connect
dup2
execve
faccessat2
fork
fstat
getdents64
getsockname
listen
lstat
open
openat
prctl
sched_process_exit
security_bprm_check
security_inode_unlink
security_socket_accept
security_socket_bind
security_socket_connect
security_socket_create
security_socket_listen
socket
stat
unlink
→ demo git:(main) 
```



```
fhir-server_1  | [8/17/21, 2:04:21:915 UTC] 0000004e FHIRServletCo I   Bypassing NATS notifi
cation init.
fhir-server_1  | [8/17/21, 2:04:21:916 UTC] 0000004e FHIRServletCo 1   Initializing FHIRRegi
stry...
fhir-server_1  | [8/17/21, 2:04:21:924 UTC] 0000004e FHIRBuildIden I   Build properties file
 successfully loaded: buildinfo.fhirserver.properties
fhir-server_1  | [8/17/21, 2:04:21:924 UTC] 0000004e FHIRBuildIden I   Build properties file
 contains:
fhir-server_1  | {fhir.server.build.version=4.9.0, fhir.server.build.id=Integration_refs/tag
s/4.9.0_d0545fbe546e1136b776ad598795f6f3e85c4ffa}
fhir-server_1  | [8/17/21, 2:04:21:924 UTC] 0000004e FHIRApplicati I   FHIR Server version 4
.9.0 build id 'Integration_refs/tags/4.9.0_d0545fbe546e1136b776ad598795f6f3e85c4ffa' startin
g.
fhir-server_1  | [8/17/21, 2:04:21:950 UTC] 0000004e cl21062021052 I   Setting the server's
publish address to be /
fhir-server_1  | [8/17/21, 2:04:21:965 UTC] 0000004e servlet       I com.ibm.ws.webcontainer
.servlet.ServletWrapper init SRVE0242I: [fhir-server-webapp] [/fhir-server/api/v4] [FHIRRest
Servlet]: Initialization successful.
fhir-server_1  | [8/17/21, 2:04:21:967 UTC] 0000004e FHIRRestServl I   Configured tenant-id
header name is: X-FHIR-TENANT-ID
fhir-server_1  | [8/17/21, 2:04:21:968 UTC] 0000004e FHIRRestServl I   Configured datastore-
id header name is: X-FHIR-DSID
fhir-server_1  | [8/17/21, 2:04:21:968 UTC] 0000004e FHIRRestServl I   Configured original-r
equest-uri header name is: X-Watson-DP-URL-in
fhir-server_1  | [8/17/21, 2:04:21:968 UTC] 0000004e FHIRRestServl I   Configured default te
nant-id value is: default
fhir-server_1  | [8/17/21, 2:04:21:968 UTC] 0000004e AppMessageHel A   CWWKZ0001I: Applicati
on fhir-server-webapp started in 3.482 seconds.
fhir-server_1  | [8/17/21, 2:04:21:976 UTC] 00000033 TCPPort       I   CWWKO0219I: TCP Chann
el defaultHttpEndpoint has been started and is now listening for requests on host *  (IPv4)
port 9080.
fhir-server_1  | [8/17/21, 2:04:21:978 UTC] 00000033 TCPPort       I   CWWKO0219I: TCP Chann
el defaultHttpEndpoint-ssl has been started and is now listening for requests on host *  (IP
v4) port 9443.
fhir-server_1  | [8/17/21, 2:04:21:981 UTC] 00000033 FeatureManage A   CWWKF0012I: The serve
r installed the following features: [appSecurity-2.0, appSecurity-3.0, batch-1.0, batchManag
ement-1.0, cdi-2.0, distributedMap-1.0, el-3.0, jaxrs-2.1, jaxrsClient-2.1, jdbc-4.1, jndi-1
.0, json-1.0, jsonp-1.1, jwt-1.0, localConnector-1.0, mpConfig-2.0, mpJwt-1.2, mpOpenAPI-2.0
, servlet-4.0, ssl-1.0, transportSecurity-1.0, websocket-1.1].
fhir-server_1  | [8/17/21, 2:04:21:982 UTC] 00000033 FeatureManage I   CWWKF0008I: Feature u
pdate completed in 4.370 seconds.
fhir-server_1  | [8/17/21, 2:04:21:982 UTC] 00000033 FeatureManage A   CWWKF0011I: The defau
ltServer server is ready to run a smarter planet. The defaultServer server started in 5.532
seconds.
fhir-server_1  | [8/17/21, 2:04:21:985 UTC] 00000048 PluginGenerat I   SRVE9103I: A configur
ation file for a web server plugin was automatically generated for this server at /opt/ol/wl
p/output/defaultServer/logs/state/plugin-cfg.xml.
```

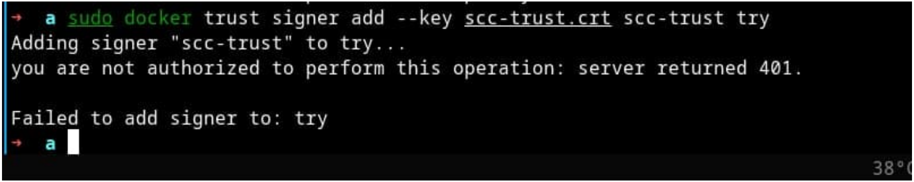
```
→  demo git:(main) sudo docker exec -it -u 0 demo_fhir-server_1 bash
[root@fhir defaultServer]# ls -l
total 144
drwxr-xr-x 1 default root  4096 Aug 11 20:34 apps
-rw-r--r-- 1 default root   148 Aug 11 19:28 bootstrap.properties
drwxr-xr-x 3    1000 1000  4096 Aug 16 23:33 config
drwxr-xr-x 1 default root  4096 Aug 11 19:28 configDropins
drwxr-xr-x 2 default root  4096 Aug 11 20:25 docs
drwxrwx--- 1 default root  4096 Jul 19 22:11 dropins
-rw-r--r-- 1 default root 90808 Aug 17 02:04 fhirschema.log
-rwxr-xr-x 1 default root   888 Aug 11 19:28 jvm.options
drwxr-xr-x 3 default root  4096 Aug 11 19:28 resources
-rwxr-xr-x 1 default root     6 Aug 11 19:28 server.env
-rwxr-xr-x 1 default root  6030 Aug 11 19:28 server.xml
drwxr-xr-x 2    1000 1000  4096 Aug 16 23:33 userlib
[root@fhir defaultServer]# chown 1000:1000 docs
chown: changing ownership of 'docs': Operation not permitted
[root@fhir defaultServer]# █
```

```
▢ 0  ↑ 1d 11h 47m  1 zsh  2 sudo  3 zsh                    39.6667°C | 10:04 | 17 Aug  root!  scc-lab
```



```
ng recovery log files found in /opt/ol/wlp/output/defaultServer/tranlog/tranlog. Cold starti
ng the recovery log.
fhir-server_1  | [8/17/21, 2:06:08:755 UTC] 00000073 LogFileHandle I   CWRLS0006I: Creating
new recovery log file /opt/ol/wlp/output/defaultServer/tranlog/tranlog/log1.
fhir-server_1  | [8/17/21, 2:06:08:759 UTC] 00000073 LogFileHandle I   CWRLS0006I: Creating
new recovery log file /opt/ol/wlp/output/defaultServer/tranlog/tranlog/log2.
fhir-server_1  | [8/17/21, 2:06:08:826 UTC] 00000073 LogHandle     I   CWRLS0007I: No existi
ng recovery log files found in /opt/ol/wlp/output/defaultServer/tranlog/partnerlog. Cold sta
rting the recovery log.
fhir-server_1  | [8/17/21, 2:06:08:827 UTC] 00000073 LogFileHandle I   CWRLS0006I: Creating
new recovery log file /opt/ol/wlp/output/defaultServer/tranlog/partnerlog/log1.
fhir-server_1  | [8/17/21, 2:06:08:829 UTC] 00000073 LogFileHandle I   CWRLS0006I: Creating
new recovery log file /opt/ol/wlp/output/defaultServer/tranlog/partnerlog/log2.
fhir-server_1  | [8/17/21, 2:06:08:866 UTC] 00000058 RecoveryDirec I   CWRLS0012I: All persi
stent services have been directed to perform recovery processing for this WebSphere server (
defaultServer).
fhir-server_1  | [8/17/21, 2:06:08:866 UTC] 00000073 RecoveryManag I   WTRN0135I: Transactio
n service recovering no transactions.
fhir-server_1  | [8/17/21, 2:06:08:882 UTC] 00000058 ConnectorServ I   J2CA8050I: An authent
ication alias should be used instead of defining a user name and password on dataSource[fhir
DatasourceDefaultDefault].
fhir-server_1  | [8/17/21, 2:06:08:951 UTC] 00000058 FHIRDbDAOImpl 1   Getting connection fo
r tenantId/dsId: [default/default]...
fhir-server_1  | [8/17/21, 2:06:09:008 UTC] 00000058 DatabaseHelpe I   DSRA8203I: Database p
roduct name : PostgreSQL
fhir-server_1  | [8/17/21, 2:06:09:009 UTC] 00000058 DatabaseHelpe I   DSRA8204I: Database p
roduct version : 12.6
fhir-server_1  | [8/17/21, 2:06:09:009 UTC] 00000058 DatabaseHelpe I   DSRA8205I: JDBC drive
r name  : PostgreSQL JDBC Driver
fhir-server_1  | [8/17/21, 2:06:09:009 UTC] 00000058 DatabaseHelpe I   DSRA8206I: JDBC drive
r version  : 42.2.18
fhir-server_1  | [8/17/21, 2:06:09:023 UTC] 00000058 FHIRDbConnect 1   Configuring new conne
ction in this transaction. Key='com.ibm.fhir.persistence.jdbc.connection.FHIRDbTenantDatasou
rceConnectionStrategy/default/default'
fhir-server_1  | [8/17/21, 2:06:09:023 UTC] 00000058 FHIRDbDAOImpl 1   Got the connection fo
r [default/default]. Took 72 ms
fhir-server_1  | [8/17/21, 2:06:09:025 UTC] 00000058 FHIRUserTrans 1   Committing transactio
n on current thread...
fhir-server_1  | [8/17/21, 2:06:09:026 UTC] 00000058 FHIRPersisten 1   Transaction committed
 - updating cache shared maps
fhir-server_1  | [8/17/21, 2:06:09:026 UTC] 00000058 FHIRRestHelpe 1   Returned from invocat
ion of operation 'healthcheck'...
fhir-server_1  | [8/17/21, 2:06:09:031 UTC] 00000058 AuditLogServi I   Successfully initiali
zed audit log service: com.ibm.fhir.audit.impl.NopService
fhir-server_1  | [8/17/21, 2:06:09:037 UTC] 00000058 FHIRRestServl I   Completed request[0.4
34 secs]: tenantId:[default] dsId:[default] user:[fhiruser] method:[GET] uri:[https://localh
ost:9443/fhir-server/api/v4/$healthcheck] status:[200]
```

```
total 144
drwxr-xr-x 1 default root  4096 Aug 11 20:34 apps
-rw-r--r-- 1 default root   148 Aug 11 19:28 bootstrap.properties
drwxr-xr-x 3    1000 1000  4096 Aug 16 23:33 config
drwxr-xr-x 1 default root  4096 Aug 11 19:28 configDropins
drwxr-xr-x 2 default root  4096 Aug 11 20:25 docs
drwxrwx--- 1 default root  4096 Jul 19 22:11 dropins
-rw-r--r-- 1 default root 90808 Aug 17 02:04 fhirschema.log
-rwxr-xr-x 1 default root   888 Aug 11 19:28 jvm.options
drwxr-xr-x 3 default root  4096 Aug 11 19:28 resources
-rwxr-xr-x 1 default root     6 Aug 11 19:28 server.env
-rwxr-xr-x 1 default root  6030 Aug 11 19:28 server.xml
drwxr-xr-x 2    1000 1000  4096 Aug 16 23:33 userlib
[root@fhir defaultServer]# chown 1000:1000 docs
chown: changing ownership of 'docs': Operation not permitted
[root@fhir defaultServer]# exit
exit
→  demo git:(main) sudo docker exec -it -u 0 demo_fhir-server_1 bash
[root@fhir defaultServer]# ls -l
total 144
drwxr-xr-x 1 default root  4096 Aug 11 20:34 apps
-rw-r--r-- 1 default root   148 Aug 11 19:28 bootstrap.properties
drwxr-xr-x 3    1000 1000  4096 Aug 16 23:33 config
drwxr-xr-x 1 default root  4096 Aug 11 19:28 configDropins
drwxr-xr-x 2 default root  4096 Aug 11 20:25 docs
drwxrwx--- 1 default root  4096 Jul 19 22:11 dropins
-rw-r--r-- 1 default root 90808 Aug 17 02:05 fhirschema.log
-rwxr-xr-x 1 default root   888 Aug 11 19:28 jvm.options
drwxr-xr-x 3 default root  4096 Aug 11 19:28 resources
-rwxr-xr-x 1 default root     6 Aug 11 19:28 server.env
-rwxr-xr-x 1 default root  6030 Aug 11 19:28 server.xml
drwxr-xr-x 2    1000 1000  4096 Aug 16 23:33 userlib
[root@fhir defaultServer]# chown 1000:1000 docs
[root@fhir defaultServer]# ls -l
total 144
drwxr-xr-x 1 default root  4096 Aug 11 20:34 apps
-rw-r--r-- 1 default root   148 Aug 11 19:28 bootstrap.properties
drwxr-xr-x 3    1000 1000  4096 Aug 16 23:33 config
drwxr-xr-x 1 default root  4096 Aug 11 19:28 configDropins
drwxr-xr-x 1    1000 1000  4096 Aug 11 20:25 docs
drwxrwx--- 1 default root  4096 Jul 19 22:11 dropins
-rw-r--r-- 1 default root 90808 Aug 17 02:05 fhirschema.log
-rwxr-xr-x 1 default root   888 Aug 11 19:28 jvm.options
drwxr-xr-x 3 default root  4096 Aug 11 19:28 resources
-rwxr-xr-x 1 default root     6 Aug 11 19:28 server.env
-rwxr-xr-x 1 default root  6030 Aug 11 19:28 server.xml
drwxr-xr-x 2    1000 1000  4096 Aug 16 23:33 userlib
[root@fhir defaultServer]#
```



```
→  a sudo docker trust signer add --key scc-trust.crt scc-trust try
Adding signer "scc-trust" to try...
you are not authorized to perform this operation: server returned 401.

Failed to add signer to: try
→  a 
```

38°

https://docs.docker.com/registry/deploying/