The Container Security in Healthcare Data Exchange System

Bachelor's degree graduation project

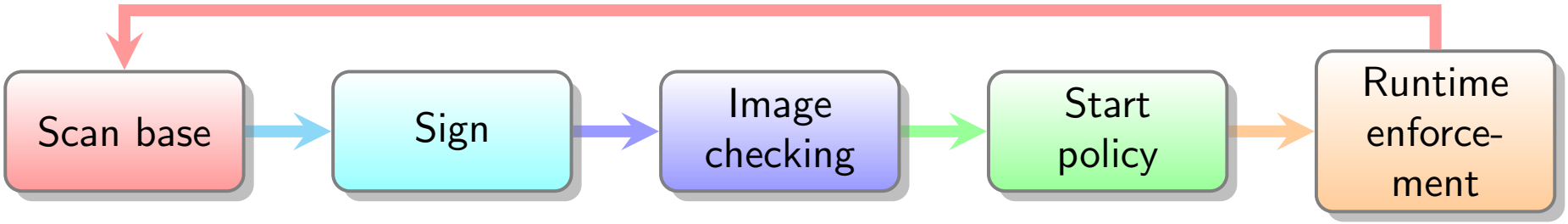
Chih-Hsuan Yang

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

September 10, 2021

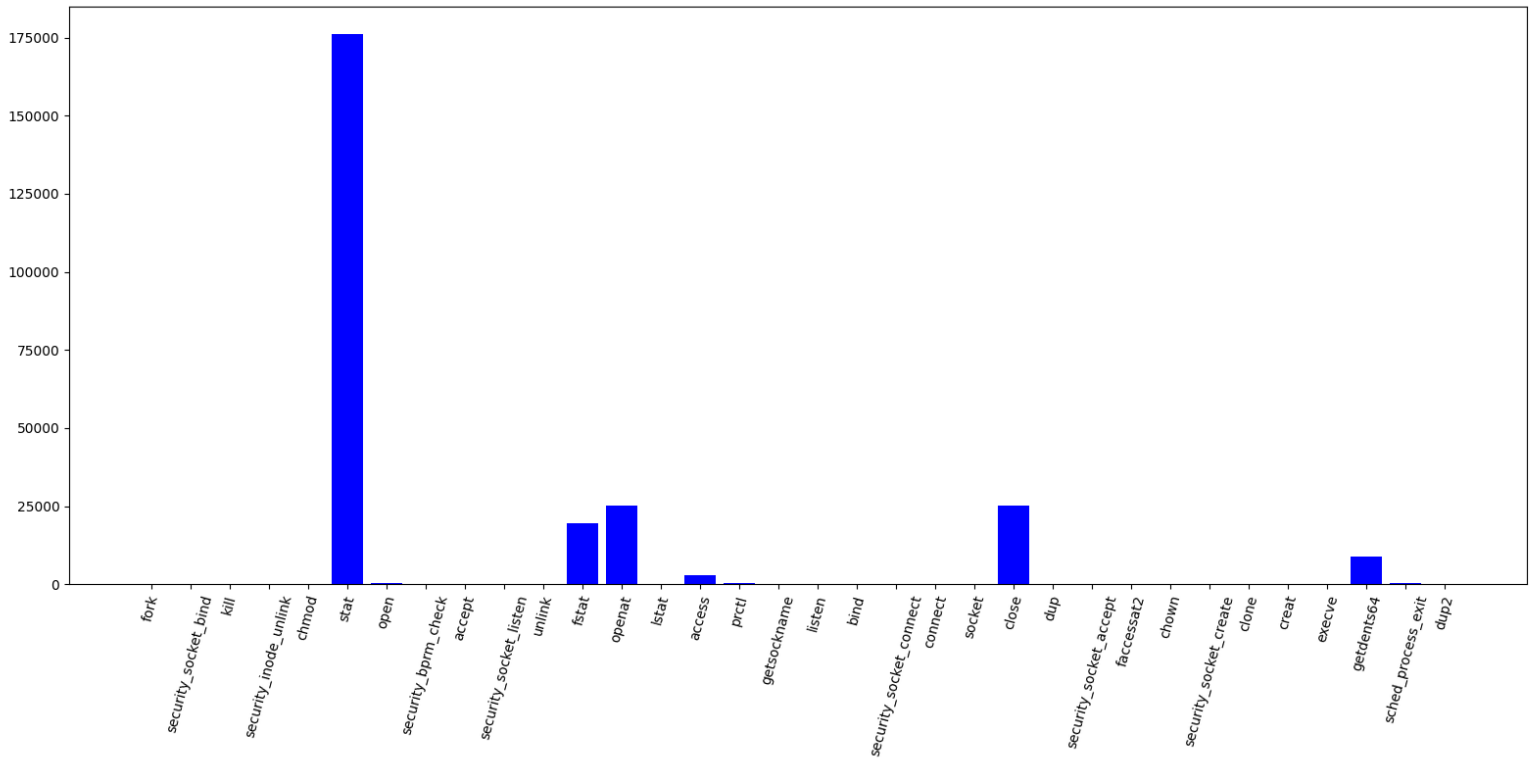
Outline

Flow chart


Scan base
Sign
Image checking
Start policy
Runtime enforce-ment

TL;DR

Current state



Current state

```
➜  demo git:(ae7adb2cbe) cat /mnt/out | jq '.eventName'| awk '{count[$0]++} END {for (word in count) print word, count[word]}'
"fork" 29
"security_socket_bind" 4
"kill" 2
"security_inode_unlink" 91
"chmod" 23
"stat" 176168
"open" 489
"security_bprm_check" 179
"accept" 18
"security_socket_listen" 4
"unlink" 64
"fstat" 19613
"openat" 25306
"lstat" 104
"access" 2758
"prctl" 236
"getsockname" 110
"listen" 4
"bind" 4
"security_socket_connect" 6
"connect" 82
"socket" 117
"close" 25077
"dup" 1
"security_socket_accept" 19
"faccessat2" 20
"chown" 3
"security_socket_create" 133
"clone" 196
"creat" 3
"execve" 177
"getdents64" 8986
"sched_process_exit" 237
"dup2" 27
➜  demo git:(ae7adb2cbe)
```

Current state

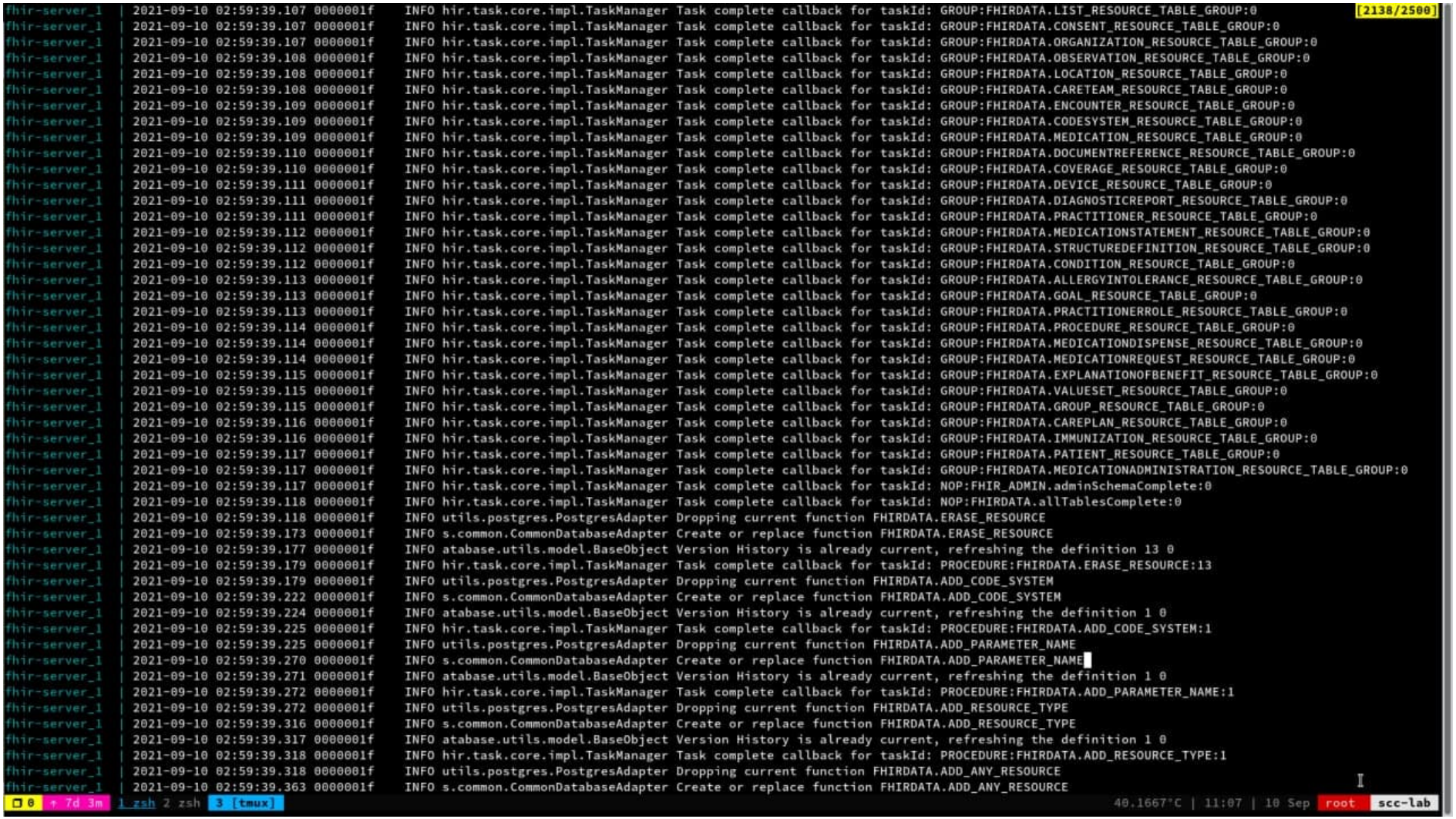
```
→  demo git:(ae7adb2cbe) cat /mnt/all_func_called| sort -k 2 -n
"dup" 1
"kill" 2
"chown" 3
"creat" 3
"bind" 4
"listen" 4
"security_socket_bind" 4
"security_socket_listen" 4
"security_socket_connect" 6
"accept" 18
"security_socket_accept" 19
"faccessat2" 20
"chmod" 23
"dup2" 27
"fork" 29
"unlink" 64
"connect" 82
"security_inode_unlink" 91
"lstat" 104
"getsockname" 110
"socket" 117
"security_socket_create" 133
"execve" 177
"security_bprm_check" 179
"clone" 196
"prctl" 236
"sched_process_exit" 237
"open" 489
"access" 2758
"getdents64" 8986
"fstat" 19613
"close" 25077
"openat" 25306
"stat" 176168
→  demo git:(ae7adb2cbe)
```

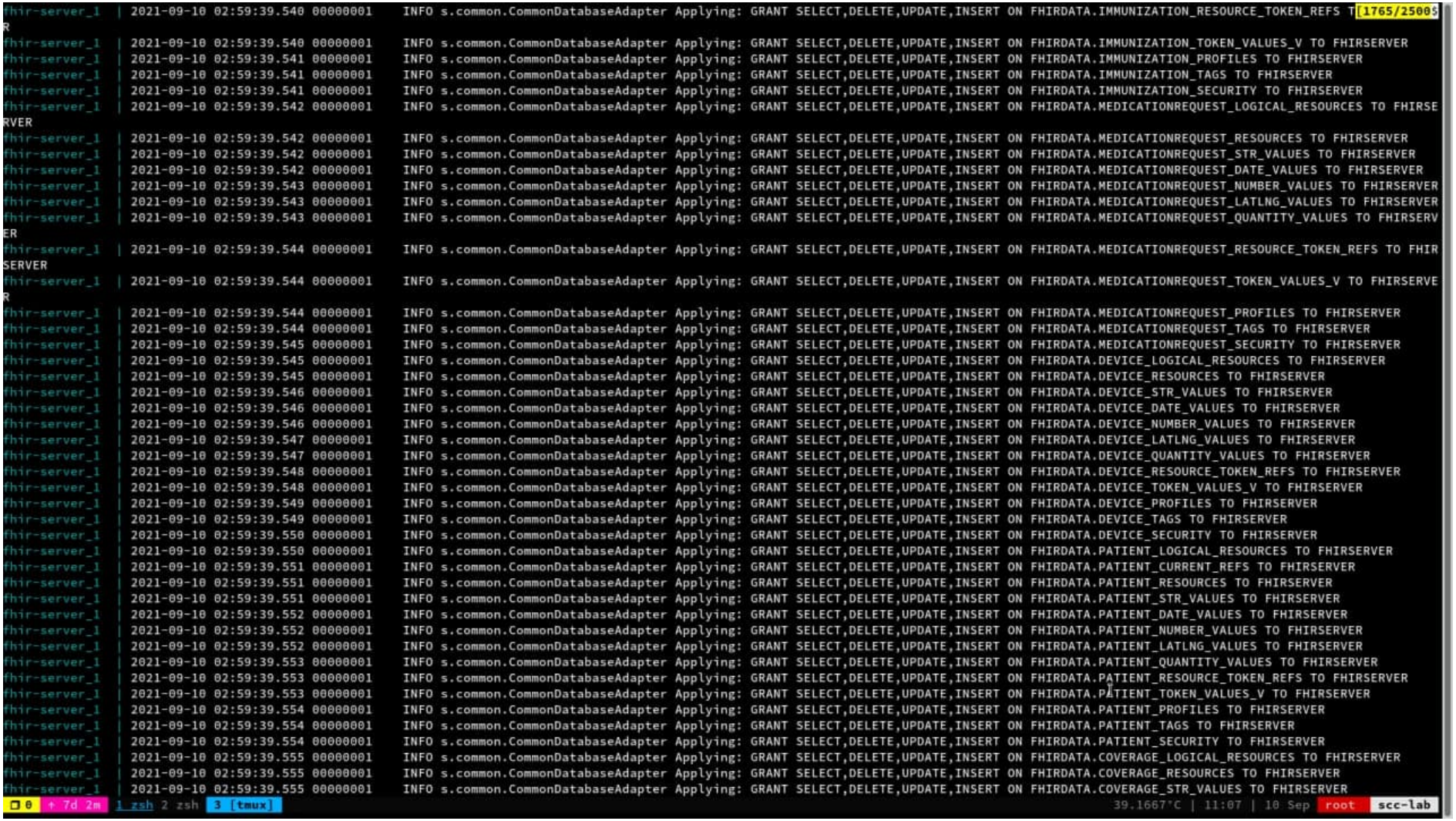
Problems

1. How to demonstrate in demo day, in paper?
   1. Might not have those attacking dataset. (Ask stavhaygn)
   2. For some specialized attacks? (BOF, DOS)?
   3. Infrastructure threats.
2. We do not reject the performance is same as the raw system.
3. Some other protection surface?

Screenshots

Unitests and intergration tests




fhir-server_1 | 2021-09-10 02:59:39.540 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.IMMUNIZATION_RESOURCE_TOKEN_REFS T[1765/25005]
R
fhir-server_1 | 2021-09-10 02:59:39.540 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.IMMUNIZATION_TOKEN_VALUES_V TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.541 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.IMMUNIZATION_PROFILES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.541 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.IMMUNIZATION_TAGS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.541 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.IMMUNIZATION_SECURITY TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.542 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_LOGICAL_RESOURCES TO FHIRSE
RVER
fhir-server_1 | 2021-09-10 02:59:39.542 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.542 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_STR_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.542 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_DATE_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.543 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_NUMBER_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.543 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_LATLNG_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.543 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_QUANTITY_VALUES TO FHIRSERV
ER
fhir-server_1 | 2021-09-10 02:59:39.544 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_RESOURCE_TOKEN_REFS TO FHIR
SERVER
fhir-server_1 | 2021-09-10 02:59:39.544 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_TOKEN_VALUES_V TO FHIRSERVE
R
fhir-server_1 | 2021-09-10 02:59:39.544 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_PROFILES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.544 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_TAGS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.545 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.MEDICATIONREQUEST_SECURITY TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.545 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_LOGICAL_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.545 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.546 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_STR_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.546 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_DATE_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.546 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_NUMBER_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.547 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_LATLNG_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.547 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_QUANTITY_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.548 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_RESOURCE_TOKEN_REFS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.548 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_TOKEN_VALUES_V TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.549 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_PROFILES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.549 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_TAGS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.550 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.DEVICE_SECURITY TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.550 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_LOGICAL_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.551 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_CURRENT_REFS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.551 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.551 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_STR_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.552 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_DATE_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.552 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_NUMBER_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.552 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_LATLNG_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.553 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_QUANTITY_VALUES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.553 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_RESOURCE_TOKEN_REFS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.553 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_TOKEN_VALUES_V TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.554 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_PROFILES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.554 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_TAGS TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.554 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.PATIENT_SECURITY TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.555 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.COVERAGE_LOGICAL_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.555 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.COVERAGE_RESOURCES TO FHIRSERVER
fhir-server_1 | 2021-09-10 02:59:39.555 00000001 INFO s.common.CommonDatabaseAdapter Applying: GRANT SELECT,DELETE,UPDATE,INSERT ON FHIRDATA.COVERAGE_STR_VALUES TO FHIRSERVER
0 ↑ 7d 2m 1 zsh 2 zsh 3 [tmux]
39.1667°C | 11:07 | 10 Sep root scc-lab

Curl

```
curl -X POST "http://localhost:9080/fhir-server/api/v4/AllergyIntolerance" -H "accept: */*" -H "Content-Type: application/fhir+json" -d "{\"resourceType\":\"AllergyIntolerance\",\"meta\":{\"tag\":[{\"code\":\"ibm/minimal\"}]},\"clinicalStatus\":{\"coding\":[{\"extension\":[{\"url\":\"http://hl7.org/fhir/StructureDefinition/data-absent-reason\",\"valueCode\":\"unknown\"}]}]},\"patient\":{\"extension\":[{\"url\":\"http://hl7.org/fhir/StructureDefinition/data-absent-reason\",\"valueCode\":\"unknown\"}]}}"
```

Request URL

```
http://localhost:9080/fhir-server/api/v4/AllergyIntolerance
```

Server response

Code	Details
201	Response headers

```
access-control-allow-origin: *
content-language: en-US
content-length: 0
date: Fri, 10 Sep 2021 03:05:32 GMT
etag: W/"1"
last-modified: Fri, 10 Sep 2021 03:05:32 GMT
location: http://localhost:9080/fhir-server/api/v4/AllergyIntolerance/17bcdaadef1-dd1fb85f-c766-4d8d-86ae-0de428cdf5df/_history/1
```

Responses

Code	Description	Links
201	Create AllergyIntolerance operation successful	*No links*

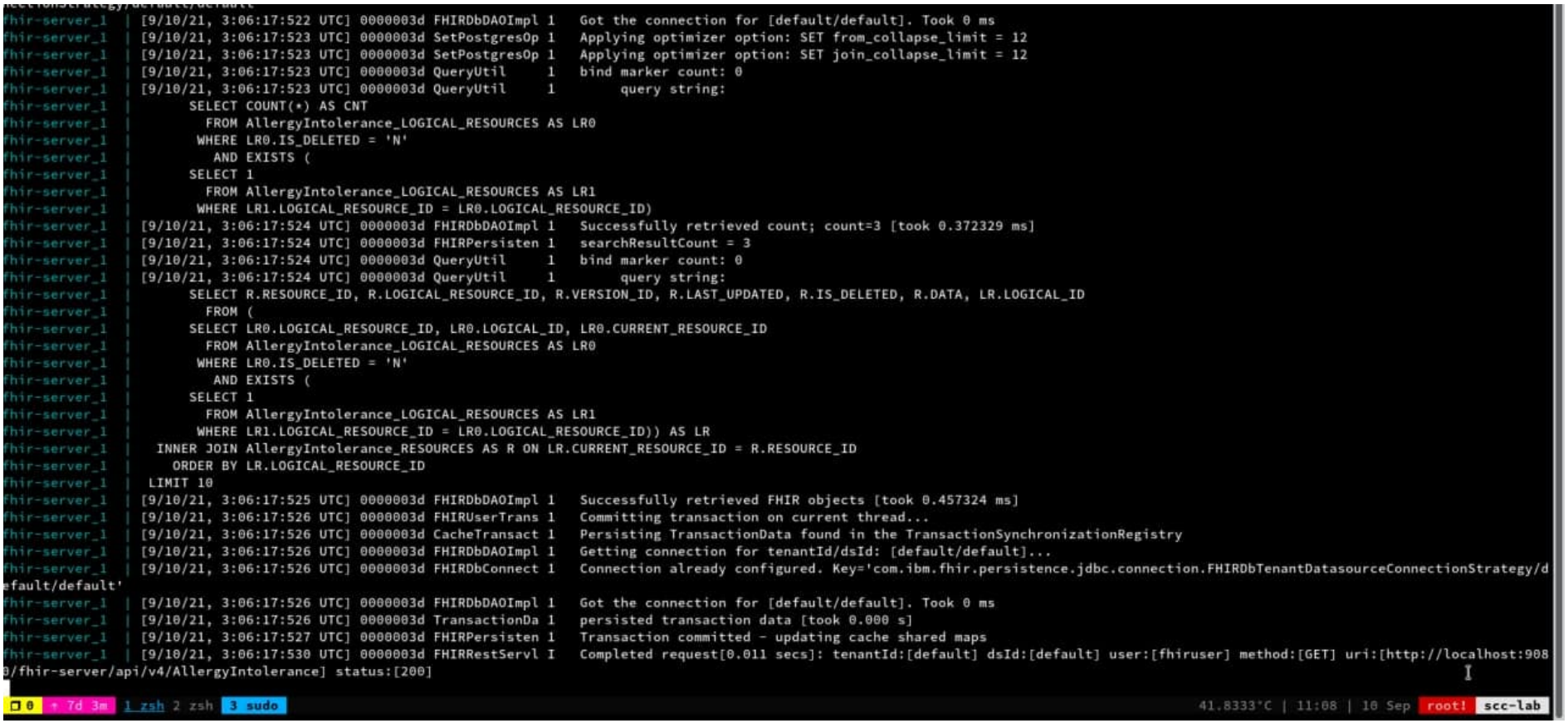
Request URL

```
http://localhost:9080/fhir-server/api/v4/AllergyIntolerance
```

Server response

Code	Details
200	Response body


```
{
  "resourceType": "Bundle",
  "id": "70008962-139e-4106-b450-233ab65acf42",
  "type": "searchset",
  "total": 3,
  "link": [
    {
      "relation": "self",
      "url": "http://localhost:9080/fhir-server/api/v4/AllergyIntolerance?_count=10&_page=1"
    }
  ],
  "entry": [
    {
      "id": "17bcc763621-b978d70d-d2a7-4ada-b62e-1ab033a7ec96",
      "fullUrl": "http://localhost:9080/fhir-server/api/v4/AllergyIntolerance/17bcc763621-b978d70d-d2a7-4ada-b62e-1ab033a7ec96",
      "resource": {
        "resourceType": "AllergyIntolerance",
        "id": "17bcc763621-b978d70d-d2a7-4ada-b62e-1ab033a7ec96",
        "meta": {
```


fhir-server_1 | [9/10/21, 3:06:17:522 UTC] 0000003d FHIRDbDAOImpl 1 Got the connection for [default/default]. Took 0 ms
fhir-server_1 | [9/10/21, 3:06:17:523 UTC] 0000003d SetPostgresOp 1 Applying optimizer option: SET from_collapse_limit = 12
fhir-server_1 | [9/10/21, 3:06:17:523 UTC] 0000003d SetPostgresOp 1 Applying optimizer option: SET join_collapse_limit = 12
fhir-server_1 | [9/10/21, 3:06:17:523 UTC] 0000003d QueryUtil 1 bind marker count: 0
fhir-server_1 | [9/10/21, 3:06:17:523 UTC] 0000003d QueryUtil 1 query string:
fhir-server_1 | SELECT COUNT(*) AS CNT
fhir-server_1 | FROM AllergyIntolerance_LOGICAL_RESOURCES AS LR0
fhir-server_1 | WHERE LR0.IS_DELETED = 'N'
fhir-server_1 | AND EXISTS (
fhir-server_1 | SELECT 1
fhir-server_1 | FROM AllergyIntolerance_LOGICAL_RESOURCES AS LR1
fhir-server_1 | WHERE LR1.LOGICAL_RESOURCE_ID = LR0.LOGICAL_RESOURCE_ID)
fhir-server_1 | [9/10/21, 3:06:17:524 UTC] 0000003d FHIRDbDAOImpl 1 Successfully retrieved count; count=3 [took 0.372329 ms]
fhir-server_1 | [9/10/21, 3:06:17:524 UTC] 0000003d FHIRPersisten 1 searchResultCount = 3
fhir-server_1 | [9/10/21, 3:06:17:524 UTC] 0000003d QueryUtil 1 bind marker count: 0
fhir-server_1 | [9/10/21, 3:06:17:524 UTC] 0000003d QueryUtil 1 query string:
fhir-server_1 | SELECT R.RESOURCE_ID, R.LOGICAL_RESOURCE_ID, R.VERSION_ID, R.LAST_UPDATED, R.IS_DELETED, R.DATA, LR.LOGICAL_ID
fhir-server_1 | FROM (
fhir-server_1 | SELECT LR0.LOGICAL_RESOURCE_ID, LR0.LOGICAL_ID, LR0.CURRENT_RESOURCE_ID
fhir-server_1 | FROM AllergyIntolerance_LOGICAL_RESOURCES AS LR0
fhir-server_1 | WHERE LR0.IS_DELETED = 'N'
fhir-server_1 | AND EXISTS (
fhir-server_1 | SELECT 1
fhir-server_1 | FROM AllergyIntolerance_LOGICAL_RESOURCES AS LR1
fhir-server_1 | WHERE LR1.LOGICAL_RESOURCE_ID = LR0.LOGICAL_RESOURCE_ID)) AS LR
fhir-server_1 | INNER JOIN AllergyIntolerance_RESOURCES AS R ON LR.CURRENT_RESOURCE_ID = R.RESOURCE_ID
fhir-server_1 | ORDER BY LR.LOGICAL_RESOURCE_ID
fhir-server_1 | LIMIT 10
fhir-server_1 | [9/10/21, 3:06:17:525 UTC] 0000003d FHIRDbDAOImpl 1 Successfully retrieved FHIR objects [took 0.457324 ms]
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d FHIRUserTrans 1 Committing transaction on current thread...
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d CacheTransact 1 Persisting TransactionData found in the TransactionSynchronizationRegistry
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d FHIRDbDAOImpl 1 Getting connection for tenantId/dsId: [default/default]...
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d FHIRDbConnect 1 Connection already configured. Key='com.ibm.fhir.persistence.jdbc.connection.FHIRDbTenantDatasourceConnectionStrategy/default/default'
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d FHIRDbDAOImpl 1 Got the connection for [default/default]. Took 0 ms
fhir-server_1 | [9/10/21, 3:06:17:526 UTC] 0000003d TransactionDa 1 persisted transaction data [took 0.000 s]
fhir-server_1 | [9/10/21, 3:06:17:527 UTC] 0000003d FHIRPersisten 1 Transaction committed - updating cache shared maps
fhir-server_1 | [9/10/21, 3:06:17:530 UTC] 0000003d FHIRRestServl I Completed request[0.011 secs]: tenantId:[default] dsId:[default] user:[fhiruser] method:[GET] uri:[http://localhost:9080/fhir-server/api/v4/AllergyIntolerance] status:[200]
0 7d 3m 1 zsh 2 zsh 3 sudo
41.8333°C | 11:08 | 10 Sep root! scc-lab

STDIN


```
{
  "timestamp": 1631242658000505000,
  "processId": 22,
  "threadId": 22,
  "parentProcessId": 1,
  "hostProcessId": 3704142,
  "hostThreadId": 3704142,
  "hostParentProcessId": 3704058,
  "userId": 0,
  "mountNamespace": 4026532858,
  "pidNamespace": 4026532861,
  "processName": "bash",
  "hostName": "fhir",
  "containerId": "",
  "eventId": "59",
  "eventName": "execve",
  "argsNum": 2,
  "returnValue": 0,
  "stackAddresses": null,
  "args": [
    {
      "name": "pathname",
      "type": "const char*",
      "value": "/usr/bin/basename"
    },
    {
      "name": "argv",
      "type": "const char*const*",
      "value": [
        "basename",
        "/opt/ibm-fhir-server/bootstrap.sh"
      ]
    }
  ]
}
{
  "timestamp": 1631242658000637400,
  "processId": 22,
  "threadId": 22,
  "parentProcessId": 1,
  "hostProcessId": 3704142,
  "hostThreadId": 3704142,
```


```
➜  0910 git:(main) ✗ cat /mnt/out | jq | bat -l json
➜  0910 git:(main) ✗ ll -h /mnt/out
-rw-r--r-- 1 root root 143M Sep 10 11:08 /mnt/out
➜  0910 git:(main) ✗
```

Problems

1. How to demonstrate in demo day, in paper?
   1. Might not have those attacking dataset. (Ask stavhaygn)
   2. For some specialized attacks? (BOF, DOS)?
   3. Infrastructure threats.
2. We do not reject the performance is same as the raw system.
3. Some other protection surface?