OAK RIDGE National Laboratory

Channel Access Security Lab

John Sinclair,
Kay Kasemir

Jan/Feb. 2022

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

Procedure

- Run a database with "..:ramp" and "..:limit" records
- Note that there are no restrictions on modifying ..:limit
- Reconfigure the IOC to use access security
- Assert that only user "expert" may modify the above PV when security is enabled
- Disable access security and verify no restrictions

Open two terminal windows

Window 1 – run IOC

- cd /ics/examples/11_casecurity

Read database and run it

- gedit demo.db &
- softIoc –m S=demo –d demo.db

Check who's connected

- casr 1

Verify that there is no acc.sec.

- asdbdump

Window 2 – access it

- camonitor demo:ramp

Ctrl-C to stop camonitor, then

- caput demo:limit 5

Note that write succeeds

- caget demo:limit
- camonitor demo:ramp

Add Access Security

Window 1 – run IOC

- cd /ics/examples/11_casecurity

Check what we're running

- gedit demo.db secure.acf &
- softIoc –m S=demo –d demo.db –a secure.acf

Check who's connected

- casr 1

Verify that acc.sec. rules are defined

- asdbdump

Window 2 – access it

- camonitor demo:ramp

Note that write still succeeds

- caput demo:limit 5
- caget demo:limit
- camonitor demo:ramp

Explain why!

Enable Access Security

Window 1 – Update databse & run IOC

- cd /ics/examples/11_casecurity

Check “ACF” comments and fix database

- gedit solution.db secure.acf &
- softIoc –m S=demo –d solution.db –a secure.acf

Check who’s connected

- casr 1

Verify that acc.sec. rules are defined

- asdbdump

Window 2 – access it

- camonitor demo:ramp

Enable Access Security .. and test it

Window 3 (new)

Verify that the “training” user can no longer write

- caput demo:limit 5

Change the mode, check we can write in that state

- caput demo:accessState 1
- caput demo:limit 5

Back to normal

- caput demo:accessState 0
- caput demo:limit 10

Enable Access Security .. and test it

Window 3

Change to ”expert” (password is $expert), check if that user can write

- su expert
- caput demo:limit 5

Check if that is independent from the “demo:accessState”

Check with GUI

Create a display.

Note how the text entry for demo:limit changes based on mode

Note

- We used ‘softIoc’ and its ’-a /path/to/config.asg’ option.
- Run with added option ‘-v’ to see what would go into the st.cmd of a makeBaseApp IOC

```
$ softIoc -v -m S=demo -a secure.acf -d solution.db
…
asSetSubstitutions("S=demo")
asSetFilename("secure.acf")
…
dbLoadRecords("solution.db", "S=demo")
iocInit()
```