**QEMU**

To debug OP-TEE when using QEMU you could use gdb as the main debugger.

Step1:**(https://github.com/OP-TEE/build)**

Install repo if it is not present in your system by using

$ sudo apt-get install repo  
Step2:

If any error came while installing repo about username and mail id register

username and mai id as given commands when run above command

Step3:

create a directory in your home folder with name qemu

$ mkdir qemu

$cd qemu

Step4:

In that directory download qemu by using following

$ repo init -u https://github.com/OP-TEE/manifest.git -m qemu\_v8.xml

step5:

after successfull downloading qemu by using step4 run fulowing command

$repo sync

step5:

after repo sync run make toolchains for the purpose of downloading tool chains

$ cd build

$ make toolchains

step 6:

after downloading toolchains build the source code by using make

$ make

step 7:

after make successfull run make run only

$make run only

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

step8:(https://github.com/OP-TEE/build/blob/master/docs/debug.md)

In your home directory create a file with name .gdbinit

$ vim .gdbinit

in his file following code write

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

set print array on

set print pretty on

define optee

handle SIGTRAP noprint nostop pass

symbol-file $HOME/devel/optee/optee\_os/out/arm/core/tee.elf

target remote localhost:1234

end

document optee

Loads and setup the binary (tee.elf) for OP-TEE and also connects to the QEMU

remote.

End

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

In above code keep the path of tee.elf fie instead of following path

$HOME/devel/optee/optee\_os/out/arm/core/tee.elf

In Optee folder(trust zone os ) go given path run following

optee/toolchains/aarch64/bin$ ./aarch64-linux-gnu-gdb -q

(gdb) optee

SIGTRAP is used by the debugger.

Are you sure you want to change it? (y or n) [answered Y; input not from

terminal]

0x00000000 in ?? ()

(gdb) b tee\_entry\_std

Breakpoint 1 at 0x7df0c7be: file core/arch/arm/tee/entry\_std.c, line 268.

and then start the execution by writing the continue command in gdb.

(gdb) c

Continuing.

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

Now a terminal open and connected to optee from qemu in that run our applications which are there in optee\_examples.