libqtest and libqos

Nassim Eddequiouaq

March 4, 2014

QEMU: Quick QEMUlator

- Free and open-source hypervisor
- Performs hardware virtualization
- Can also be used for pure CPU emulation

Add and run your test in QEMU

Reverse Engineering skills needed:

```
> check-qtest-<YOUR_ARCH>-y += tests/<YOUR_TEST>$(EXESUF)

> tests/<YOUR_TEST>$(EXESUF): tests/<YOUR_TEST>.o $(libqos-pc-obj-y)

> make check-qtest-<YOUR_ARCH>

> QTEST_QEMU_BINARY=./<YOUR_ARCH>-softmmu/qemu-system-<YOUR_ARCH> tests/<YOUR_TEST>
```

Libqtest: Which purpose ?

- Unit testing in QEMU
- Driver/Module development
- Each test case runs as a separate process
- Full access to QEMU libc and does't need cross compiler to build

Libqtest: Content

- Start/End test: qtest_start(qemu_args) / qtest_end()
- Functions using QMP to send messages to QEMU
- IRQ/PIO/MMIO/Clock related functions
- get_arch() and add_arch(): USEFUL++

Libqos: Which purpose ?

- Aims to provide device driver framework
- Allows to write PCI, I2C, fw_cfg and other device tests
- Really bad shape at the moment: GSOC 2014

Libqos: Content

- Some OS related functions are present in libqos:
  - PCI module
  - Memory allocator module
- Several funny things:

```
static void pc_free(QGuestAllocator *allocator,
    uint64_t addr)
{
}
```

`alloc = malloc(size) and free = malloc(address)`

- Check the implementation before using a function

Libqos: Future expectations

- Virtio support: needs virtio-pci and virtio-mmio
- USB support: needs ad USB Host Controller driver
- Several other device test cases

Link

- http://git.qemu.org/git/qemu.git
- http://qemu-project.org/Google_Summer_of_Code_2014
- https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git