Features/VirtioCrypto

The virtio crypto is a virtual crypto device as well as a kind of virtual hardware accelerator for virtual machines. The encryption and decryption requests are placed in the data queue and handled by the real crypto accelerators finally. The second queue is the control queue used to create or destroy sessions for symmetric algorithms and control some advanced features in the future. The virtio crypto device provides the following crypto services: CIPHER, MAC, HASH, AEAD etc.

Contents

Feature maintainers

Gonglei: <arei.gonglei@huawei.com>

Code

- Virtio-crypto specification: Gonglei's virtio.git (https://github.com/gongleiarei/virtio)
- Virtio-crypto linux driver: Gonglei's virtio-crypto-linux-driver.git (https://github.com/gongleiarei/virtio-crypto-linux-driver)
- QEMU: Gonglei's qemu.git (https://github.com/gongleiarei/qemu/tree/virtio-crypto)
- Cryptodev-linux: Cryptodev-linux's website (http://cryptodev-linux.org/) Cryptodev-linux is implemented as a standalone module that requires no dependencies other than a stock linux kernel.

Quickstart

Host:

- Step 1: Build Qemu with **gcrypt** or **nettle** cryptography support

```
$ git clone -b virtio-crypto https://github.com/gongleiarei/qemu
$ cd qemu
$ ./configure --target-list=x86_64-softmmu
$ make
```

- Step 2: Strat Qemu using the following parameters:

```
$ qemu-system-x86_64 \
   [...] \
       -object cryptodev-backend-builtin,id=cryptodev0 \
       -device virtio-crypto-pci,id=crypto0,cryptodev=cryptodev0 \
   [...]
```

Guest:

- Step 1: get the newest virtio-crypto linux driver which was merged in Linux master tree.

```
 $ git clone https://github.com/torvalds/linux.git
 $ make; make modules_install; make install
 $ reboot; # with the newest linux kernel
```

- Step 2: use cryptodev-linux test the crypto functions

Testing

Use the cryptodev-linux module to test the crypto functions in the guest.

```
$ git clone https://github.com/cryptodev-linux/cryptodev-linux.git
$ cd cryptodev-linux
$ make; make install
$ cd tests
$ ./cipher -
requested cipher CRYPTO_AES_CBC, got cbc(aes) with driver virtio_crypto_aes_cbc
AES Test passed
requested cipher CRYPTO_AES_CBC, got cbc(aes) with driver virtio_crypto_aes_cbc
requested cipher CRYPTO_AES_CBC, got cbc(aes) with driver virtio_crypto_aes_cbc
Test passed
```

A simple benchmark in the cryptodev-linux module (synchronous encryption in the guest and no hardware accelerator in the host)

```
$ ./speed
 Testing AES-128-CBC cipher:
      Encrypting in chunks of 512 bytes: done. 85.10 MB in 5.00 secs: 17.02 MB/sec
      Encrypting in chunks of 1024 bytes: done. 162.98 MB in 5.00 secs: 32.59 MB/sec
      Encrypting in chunks of 2048 bytes: done. 292.93 MB in 5.00 secs: 58.58 MB/sec
      Encrypting in chunks of 4096 bytes: done. 500.77 MB in 5.00 secs: 100.14 MB/sec
      Encrypting in chunks of 8192 bytes: done. 766.14 MB in 5.00 secs: 153.20 MB/sec
      Encrypting in chunks of 16384 bytes: done. 1.05 GB in 5.00 secs: 0.21 GB/sec
      Encrypting in chunks of 32768 bytes: done. 1.31 GB in 5.00 secs: 0.26 GB/sec
      Encrypting in chunks of 65536 bytes: done. 1.51 GB in 5.00 secs: 0.30 GB/sec
```

Links

- China Linux Kernel Conference 2015 presentation: A new framework of cryptography virtio driver (https://privatewiki.opnfv.org/_media/dpacc/a_new_framework_of_cryptography_virtio_driver.pdf) (pdf)

Retrieved from "https://wiki.qemu.org/index.php?title=Features/VirtioCrypto&oldid=6458"

This page was last edited on 22 December 2016, at 06:41.

Content is available under GNU Free Documentation License 1.2.
QEMU is a trademark of Fabrice Bellard.