life.augmented

How to control a RNG in userspace

How to control a RNG in userspace

Stable: 03.02.2020 - 08:42 / Revision: 03.02.2020 - 08:27

Contents

1 Purpose

Hardware random framework offers the interface to control RNG devices from userspace.
This article shows two ways to control a RNG in userspace:

- using /dev/random command to generate a random number
- using rng-tools to validate the RNG

2 RNG control through /dev/random

/dev/random is a special file that can be used to generate random numbers based on a pseudo-random generator. It uses noise collected from device drivers and hardware random sources to generate data. od (octal dump) command is used to extract the number of bytes and display the decimal number.
Ex: - Random number (0 - 255):

```
Board $> od -An -N1 -i /dev/random
        172
```

- Random number (0 - 65535):

```
Board $> od -An -N2 -i /dev/random
        20041
```

3 RNG control through rng-tools

rng_tools[1] is a set of tools related to random number generation.
rng-tools will connect to the hardware random number generator through /dev/hwrng. rngtest is a basic test that checks data using FIPS 140-2 tests[2] which is a security requirement test for cryptographic module compliance.

```
Board $> rngtest -c 100 </dev
/hwrng

rngtest 5
Copyright (c) 2004 by Henrique de Moraes Holschuh
This is free software; see the source for copying conditions.  There is NO warranty;
not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

rngtest: starting FIPS tests...
rngtest: bits received from input: 2000032
rngtest: FIPS 140-2 successes: 100
rngtest: FIPS 140-2 failures: 0
rngtest: FIPS 140-2(2001-10-10) Monobit: 0
rngtest: FIPS 140-2(2001-10-10) Poker: 0
rngtest: FIPS 140-2(2001-10-10) Runs: 0
rngtest: FIPS 140-2(2001-10-10) Long run: 0
rngtest: FIPS 140-2(2001-10-10) Continuous run: 0
rngtest: input channel speed: (min=33.154; avg=33.656; max=34.217) Kibits/s
rngtest: FIPS tests speed: (min=21.193; avg=23.180; max=23.403) Mibits/s
rngtest: Program run time: 58114432 microseconds
```

It is normal for any random generator to fail in small number of tests, but failures must not exceed around 10.

4 References

- https://git.kernel.org/pub/scm/utils/kernel/rng-tools/rng-tools.git/
- https://en.wikipedia.org/wiki/FIPS_140-2

Random Number Generator