Raspberry Pi Random Numbers

Why Random Numbers?

- Video Games
  - Want the opponent to be unpredictable in most games
- Simulations
  - Real life is unpredictable.
  - Multiple simulations require a lot of random numbers.
- Security
  - Generate entropy for encryption keys.
  - Obfuscation.

Why Hardware Random Numbers

- Computers are not typically random
  - Software-based random numbers are only pseudo-random
    - Can be reproduced knowing the state of the random number generator.
- Hardware-based random numbers use the environment.
  - Ignoring Planck Length, real life is continuous.
  - The environment varies constantly.
  - Difficult to reproduce the environment.

Turn on Random Numbers

- “`sudo apt-get dist-upgrade`”
- ”`sudo apt-get install rng-tools`”
- “`sudo rpi-update`”, reboot if necessary
- Append “`bcm2835-rng`” to /etc/modules
  - This is for Raspberry Pi 3. Older Raspberry Pis use a different Broadcom chip.
  - Use “`lsmod`” and look for lines that begin with “`bcm`”
- “`sudo modprobe bcm2835-rng`” to activate the kernel module without rebooting

Testing Random Numbers #1

- “sudo apt-get install netpbm”
- “sudo cat /dev/hwrng | rawtoppm -rgb 256 256 | pnmtopng > random$(date +%Y%m%d%H%M%S).png”
- View the resulting image. There should be no discernible pattern.

Testing Random Numbers #2

- “sudo cat /dev/hwrng | rngtest -c 1000”
- Output may have a few failures, but should only be a few
  - Truly random numbers will exhibit patterns, just not regularly

```
rngtest 2-unofficial-mt.14
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: 20000032
rngtest: FIPS 140-2 successes: 999
rngtest: FIPS 140-2 failures: 1
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: 1
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=14.361; avg=955.580;
max=9765625.000)Kibits/s
rngtest: FIPS tests speed: (min=7.660; avg=13.599;
max=14.277)Mibits/s
rngtest: Program run time: 22956872 microseconds
```

Testing Random Numbers #3 (really, really, testing them)

- "`sudo apt-get install dieharder`"
- "`sudo dd if=/dev/hwrng iflag=fullblock count=3072 bs=1024k > random.pi`"
  - WILL TAKE FOREVER!!!
  - 153 hours for this 3GB sample size
  - Can use a smaller value for "`count`" but test will not be as conclusive and may show many failures
    - I used "`count=1`" for a short test
- "dieharder -a -g 201 -f random.pi"
  - WILL TAKE AN EVEN LONGER FOREVER!!!