Analysis of randomness levels in the kernel entropy pool after boot

Peter Kotvan

FI MUNI

kotvan@mail.muni.cz

March 23, 2017

What we will discuss

1. Pseudo Random Number Generators
2. General Structure
3. Data Collection
4. Data Analysis
5. Future Plans
6. Other Works
7. Bibliography

Pseudo Random Number Generators - Applications

Applications:

- One time pads

Pseudo Random Number Generators - Applications

Applications:

- One time pads
- Cryptographic key generation

Pseudo Random Number Generators - Applications

Applications:

- One time pads
- Cryptographic key generation
- Salt

Pseudo Random Number Generators - Applications

Applications:

- One time pads
- Cryptographic key generation
- Salt
- Cryptographic nonce

Pseudo Random Number Generators (PRNGs)

Types of pseudo random number generators:

- non-cryptographic deterministic PRNGs

Pseudo Random Number Generators (PRNGs)

Types of pseudo random number generators:

- non-cryptographic deterministic PRNGs
- cryptographically secure deterministic PRNGs

Pseudo Random Number Generators (PRNGs)

Types of pseudo random number generators:

- non-cryptographic deterministic PRNGs
- cryptographically secure deterministic PRNGs
- PRNGs with entropy inputs

Linux Kernel PRNG

Basic information:

- PRNG with entropy input

Linux Kernel PRNG

Basic information:

- PRNG with entropy input
- Interfaces
  - User space: `/dev/random`

Linux Kernel PRNG

Basic information:

- PRNG with entropy input
- Interfaces
  - User space: `/dev/random`
  - User space: `/dev/urandom`

Linux Kernel PRNG

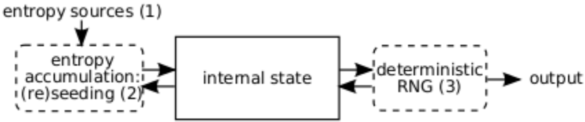
Basic information:

- PRNG with entropy input
- Interfaces
  - User space: `/dev/random`
  - User space: `/dev/urandom`
  - Kernel space: `get_random_bytes()`

Linux Kernel PRNG

Basic information:

- PRNG with entropy input
- Interfaces
  - User space: `/dev/random`
  - User space: `/dev/urandom`
  - Kernel space: `get_random_bytes()`



Entropy sources:

- Timers

Entropy sources:

- Timers
- Hardware input

Entropy sources:

- Timers
- Hardware input
- Hard drives

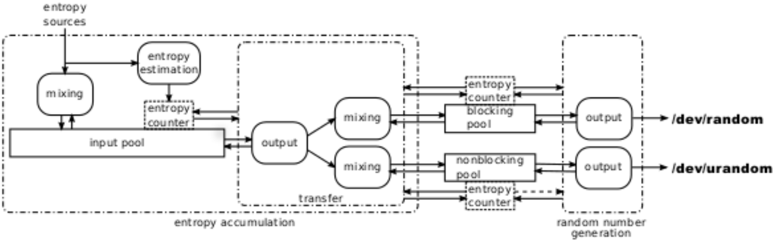
Entropy sources:

- Timers
- Hardware input
- Hard drives
- Interrupts

Entropy sources:

- Timers
- Hardware input
- Hard drives
- Interrupts
- Different hardware devices

General Structure



Entropy Collection Functions

Entropy collection:

- add_device_randomness()
- add_interrupt_randomness()
- add_timer_randomness()

Entropy Collection Functions

Entropy collection:

- `add_device_randomness()`
- `add_interrupt_randomness()`
- `add_timer_randomness()`
    - `add_input_randomness()`
    - `add_disk_randomness()`

Entropy Collection Functions

Entropy collection:

- add_device_randomness()
- add_interrupt_randomness()
- add_timer_randomness()
    - add_input_randomness()
    - add_disk_randomness()

Boot process
Input to nonblocking pool:

- add_timer_randomness()
    - add_input_randomness()
    - add_disk_randomness()
- add_interrupt_randomness()

Environment

- Linux kernel version: `3.16.1`

Environment

Environment

- Linux kernel version: `3.16.1`
- Distribution: Arch Linux

Environment

Environment

- Linux kernel version: `3.16.1`
- Distribution: Arch Linux
- Minimal kernel configuration:
    - `make localmodconfig`

Environment

- Linux kernel version: `3.16.1`
- Distribution: Arch Linux
- Minimal kernel configuration:
  - `make localmodconfig`
  - `make localyesconfig`

Kernel Patch

Data collection:

- Experimentally determine amount of data ($<$ 100KB)

Kernel Patch

Data collection:

- Experimentally determine amount of data (< 100KB)
- Data structure simple enough to parse
  - `(char *)` Function name with trailing zero character obtained by use of `__func__`

Kernel Patch

Data collection:

- Experimentally determine amount of data ($<$ 100KB)
- Data structure simple enough to parse
  - (char *) Function name with trailing zero character obtained by use of __func__
  - (size_t) Size of following data in bytes

Kernel Patch

Data collection:

- Experimentally determine amount of data (< 100KB)
- Data structure simple enough to parse
  - `(char *)` Function name with trailing zero character obtained by use of `__func__`
  - `(size_t)` Size of following data in bytes
  - Data pushed to entropy pool

Kernel Patch

Data collection:

- Experimentally determine amount of data (< 100KB)
- Data structure simple enough to parse
  - (char *) Function name with trailing zero character obtained by use of __func__
  - (size_t) Size of following data in bytes
  - Data pushed to entropy pool
- Make data available through proc file system
  - (char) large enough buffer to contain the data (200KB)

Kernel Patch

Data collection:

- Experimentally determine amount of data (< 100KB)
- Data structure simple enough to parse
  - `(char *)` Function name with trailing zero character obtained by use of `__func__`
  - `(size_t)` Size of following data in bytes
  - Data pushed to entropy pool
- Make data available through `proc` file system
  - `(char)` large enough buffer to contain the data (200KB)
  - `proc_create("prng_input", 0, NULL, &prng_input_proc_fops);`

Kernel Patch

Data collection:

- Experimentally determine amount of data (< 100KB)
- Data structure simple enough to parse
  - `(char *)` Function name with trailing zero character obtained by use of `__func__`
  - `(size_t)` Size of following data in bytes
  - Data pushed to entropy pool
- Make data available through `proc` file system
  - `(char)` large enough buffer to contain the data (200KB)
  - `proc_create("prng_input", 0, NULL, &prng_input_proc_fops);`
  - `proc_create("prng_nonblocking", 0, NULL, &prng_nonblocking_proc_fops);`

Other scripts

- Script waiting for initialization of the nonblocking pool
  parsing kernel messages - `dmesg`
  store data on drive or over network

Other scripts

- Script waiting for initialization of the nonblocking pool
  parsing kernel messages - `dmesg`
  store data on drive or over network
- `systemd` service file starting the script at the end of the boot process

Other scripts

- Script waiting for initialization of the nonblocking pool
  parsing kernel messages - `dmesg`
  store data on drive or over network
- `systemd` service file starting the script at the end of the boot process
- Script for parsing raw rata into separate directories and files
  - input pool
  - nonblocking pool

Different randomness of input data

Target - `add_device_randomness()`

Different randomness of input data

Target - `add_device_randomness()`
Two kind of entries:

- Buffer:

```
_mix_pool_bytes(&input_pool, buf, size, NULL);
```

Different randomness of input data

Target - `add_device_randomness()`
Two kind of entries:

- Buffer:

```
_mix_pool_bytes(&input_pool, buf, size, NULL);
```

- Time information:

```
unsigned long time = random_get_entropy() ^ jiffies;
_mix_pool_bytes(&input_pool, &time, sizeof(time), NULL);
```

add_device_randomness-__dev_open

```
Device information
Static/Predictable data
00000000  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
00000010  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
00000020  00 00 00 00 00 00 00 00  00 00 06 00 00 00 00 00  |................|
00000030  00 00 52 54 00 47 9d 3d  06 00 00 00 00 00 00 00  |..RT.G.=........|
00000040  00 00 00 00 00 00 06 00  00 00 00 00 00 00 52 54  |..............RT|
00000050  00 47 9d 3d 06 00 00 00  00 00 00 00 00 00 00 00  |.G.=............|
00000060  00 00 06 00 00 00 00 00  00 00 52 54 00 47 9d 3d  |..........RT.G.=|
00000070  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
00000080  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
00000090  00 00 00 00 00 00 00 00  00 00 06 00 00 00 00 00  |................|
000000a0  00 00 52 54 00 47 9d 3d  06 00 00 00 00 00 00 00  |..RT.G.=........|
000000b0  00 00 00 00 00 00 06 00  00 00 00 00 00 00 52 54  |..............RT|
000000c0  00 47 9d 3d 06 00 00 00  00 00 00 00 00 00 00 00  |.G.=............|
000000d0  00 00 06 00 00 00 00 00  00 00 52 54 00 47 9d 3d  |..........RT.G.=|
000000e0  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
000000f0  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
```

add_device_randomness-register_netdevice

```
Device information
Static/Predictable data
00000000  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
00000010  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
00000020  00 00 00 00 00 00 00 00  00 00 06 00 00 00 00 00  |................|
00000030  00 00 52 54 00 47 9d 3d  06 00 00 00 00 00 00 00  |..RT.G.=........|
00000040  00 00 00 00 00 00 06 00  00 00 00 00 00 00 52 54  |..............RT|
00000050  00 47 9d 3d 06 00 00 00  00 00 00 00 00 00 00 00  |.G.=............|
00000060  00 00 06 00 00 00 00 00  00 00 52 54 00 47 9d 3d  |..........RT.G.=|
00000070  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
00000080  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
00000090  00 00 00 00 00 00 00 00  00 00 06 00 00 00 00 00  |................|
000000a0  00 00 52 54 00 47 9d 3d  06 00 00 00 00 00 00 00  |..RT.G.=........|
000000b0  00 00 00 00 00 00 06 00  00 00 00 00 00 00 52 54  |..............RT|
000000c0  00 47 9d 3d 06 00 00 00  00 00 00 00 00 00 00 00  |.G.=............|
000000d0  00 00 06 00 00 00 00 00  00 00 52 54 00 47 9d 3d  |..........RT.G.=|
000000e0  06 00 00 00 00 00 00 00  00 00 00 00 00 00 06 00  |................|
000000f0  00 00 00 00 00 00 52 54  00 47 9d 3d 06 00 00 00  |......RT.G.=....|
```

add_device_randomness-usb_new_device

Device information

Static/Predictable data

```
00000000  0c 00 00 00 00 00 00 00  30 30 30 30 3a 30 30 3a  |........0000:00:|
00000010  30 35 2e 37 14 00 00 00  00 00 00 00 45 48 43 49  |05.7........EHCI|
00000020  20 48 6f 73 74 20 43 6f  6e 74 72 6f 6c 6c 65 72  | Host Controller|
00000030  28 00 00 00 00 00 00 00  4c 69 6e 75 78 20 33 2e  |(.......Linux 3.|
00000040  31 36 2e 31 2d 74 68 73  2d 67 33 36 66 31 37 66  |16.1-ths-g36f17f|
00000050  30 2d 64 69 72 74 79 20  65 68 63 69 5f 68 63 64  |0-dirty ehci_hcd|
00000060  0c 00 00 00 00 00 00 00  30 30 30 30 3a 30 30 3a  |........0000:00:|
00000070  30 35 2e 30 14 00 00 00  00 00 00 00 55 48 43 49  |05.0........UHCI|
00000080  20 48 6f 73 74 20 43 6f  6e 74 72 6f 6c 6c 65 72  | Host Controller|
00000090  28 00 00 00 00 00 00 00  4c 69 6e 75 78 20 33 2e  |(.......Linux 3.|
000000a0  31 36 2e 31 2d 74 68 73  2d 67 33 36 66 31 37 66  |16.1-ths-g36f17f|
000000b0  30 2d 64 69 72 74 79 20  75 68 63 69 5f 68 63 64  |0-dirty uhci_hcd|
000000c0  0c 00 00 00 00 00 00 00  30 30 30 30 3a 30 30 3a  |........0000:00:|
000000d0  30 35 2e 31 14 00 00 00  00 00 00 00 55 48 43 49  |05.1........UHCI|
000000e0  20 48 6f 73 74 20 43 6f  6e 74 72 6f 6c 6c 65 72  | Host Controller|
000000f0  28 00 00 00 00 00 00 00  4c 69 6e 75 78 20 33 2e  |(.......Linux 3.|
```

add_device_randomness-dmi_walk_early

```
Device information
Static/Predictable data
00000000  07 01 00 00 00 00 00 00  00 18 00 00 01 02 00 e8  |................|
00000010  03 00 08 00 00 00 00 00  00 00 00 04 01 00 ff ff  |................|
00000020  42 6f 63 68 73 00 42 6f  63 68 73 00 30 31 2f 30  |Bochs.Bochs.01/0|
00000030  31 2f 32 30 31 31 00 00  01 1b 00 01 01 02 00 00  |1/2011..........|
00000040  64 51 0b d0 d5 29 4b b1  95 b9 ad 20 52 4d 31 f3  |dQ...)K.... RM1.|
00000050  06 00 00 42 6f 63 68 73  00 42 6f 63 68 73 00 00  |...Bochs.Bochs..|
00000060  03 14 00 03 01 01 00 00  00 03 03 03 02 00 00 00  |................|
00000070  00 00 00 00 42 6f 63 68  73 00 00 04 20 01 04 01  |....Bochs... ...|
00000080  03 01 02 a1 06 02 00 fd  fb 8b 07 00 00 00 00 d0  |................|
00000090  07 d0 07 41 01 ff ff ff  ff ff ff 43 50 55 20 31  |...A.......CPU 1|
000000a0  00 42 6f 63 68 73 00 00  10 0f 00 10 01 03 06 00  |.Bochs..........|
000000b0  00 20 00 fe ff 01 00 00  00 11 15 00 11 00 10 02  |. ..............|
000000c0  03 40 00 40 00 00 08 09  00 01 00 07 00 00 44 49  |.@.@..........DI|
000000d0  4d 4d 20 30 00 00 13 0f  00 13 00 00 00 00 ff ff  |MM 0............|
000000e0  1f 00 00 10 01 00 00 14  13 00 14 00 00 00 00 ff  |................|
000000f0  ff 1f 00 00 11 00 13 01  00 00 00 00 20 0b 00 20  |............ .. |
```

add_device_randomness-posix_cpu_timers_exit

```
Device information
Possibly random data
00000000  08 00 00 00 00 00 00 00  88 19 00 00 00 00 00 00  |................|
00000010  08 00 00 00 00 00 00 00  da 0c 00 00 00 00 00 00  |................|
00000020  08 00 00 00 00 00 00 00  c0 09 00 00 00 00 00 00  |................|
00000030  08 00 00 00 00 00 00 00  f0 08 00 00 00 00 00 00  |................|
00000040  08 00 00 00 00 00 00 00  6a 08 00 00 00 00 00 00  |........j.......|
00000050  08 00 00 00 00 00 00 00  3b 09 00 00 00 00 00 00  |........;.......|
00000060  08 00 00 00 00 00 00 00  f3 08 00 00 00 00 00 00  |................|
00000070  08 00 00 00 00 00 00 00  ca 08 00 00 00 00 00 00  |................|
00000080  08 00 00 00 00 00 00 00  bb 08 00 00 00 00 00 00  |................|
00000090  08 00 00 00 00 00 00 00  32 09 00 00 00 00 00 00  |........2.......|
000000a0  08 00 00 00 00 00 00 00  a8 08 00 00 00 00 00 00  |................|
000000b0  08 00 00 00 00 00 00 00  f6 09 00 00 00 00 00 00  |................|
000000c0  08 00 00 00 00 00 00 00  56 09 00 00 00 00 00 00  |........V.......|
000000d0  08 00 00 00 00 00 00 00  1a 09 00 00 00 00 00 00  |................|
000000e0  08 00 00 00 00 00 00 00  cf 08 00 00 00 00 00 00  |................|
000000f0  08 00 00 00 00 00 00 00  db 08 00 00 00 00 00 00  |................|
```

Closer look - posix cpu timers exit

Statistics:

- # of entries: 932923
- # of entry classes: 655493
- # of classes / # of entries ratio: 0.702
- average # of 0x00 per entry: 5.155
- lengths of entries: 8B

Closer look - posix cpu timers exit

Statistics:

- # of entries: 932923
- # of entry classes: 655493
- # of classes / # of entries ratio: 0.702
- average # of 0x00 per entry: 5.155
- lengths of entries: 8B

`Gather more data to compute Shannons entropy`

- $2^{8*3} = 16777216$

Closer look - posix cpu timers exit

Statistics:

- # of entries: 932923
- # of entry classes: 655493
- # of classes / # of entries ratio: 0.702
- average # of 0x00 per entry: 5.155
- lengths of entries: 8B

`Gather more data to compute Shannons entropy`

- $2^{8*3} = 16777216$
- $H(X) = -\sum_i P(x_i) \log_b P(x_i)$

add_device_randomness_time-__dev_open

```
Time information
00000000  08 00 00 00 00 00 00 00  6a d6 be b9 04 00 00 00  |........j.......|
00000010  08 00 00 00 00 00 00 00  4c 7a 00 e0 06 00 00 00  |........Lz......|
00000020  08 00 00 00 00 00 00 00  3d 9b 54 bf 04 00 00 00  |........=.T.....|
00000030  08 00 00 00 00 00 00 00  f6 bf e1 7f 06 00 00 00  |................|
00000040  08 00 00 00 00 00 00 00  a1 4f 56 cb 04 00 00 00  |.........OV.....|
00000050  08 00 00 00 00 00 00 00  f4 98 a0 b7 06 00 00 00  |................|
00000060  08 00 00 00 00 00 00 00  9f 26 d9 a7 04 00 00 00  |.........&......|
00000070  08 00 00 00 00 00 00 00  47 5e 47 cc 06 00 00 00  |........G^G.....|
00000080  08 00 00 00 00 00 00 00  f5 ae 9d db 04 00 00 00  |................|
00000090  08 00 00 00 00 00 00 00  fb cb 3d 06 05 00 00 00  |..........=.....|
000000a0  08 00 00 00 00 00 00 00  bc 19 25 df 04 00 00 00  |..........%.....|
000000b0  08 00 00 00 00 00 00 00  36 52 ff e5 06 00 00 00  |........6R......|
000000c0  08 00 00 00 00 00 00 00  23 cb 13 dd 04 00 00 00  |........#.......|
000000d0  08 00 00 00 00 00 00 00  57 02 0e e7 06 00 00 00  |........W.......|
000000e0  08 00 00 00 00 00 00 00  3a a3 39 d5 04 00 00 00  |........:.9.....|
000000f0  08 00 00 00 00 00 00 00  c7 35 ab db 06 00 00 00  |.........5......|
```

add_device_randomness_time-register_netdevice

```
Time information
00000000  08 00 00 00 00 00 00 00  a9 9b 9e 55 03 00 00 00  |...........U....|
00000010  08 00 00 00 00 00 00 00  30 20 98 3d 03 00 00 00  |........0 .=....|
00000020  08 00 00 00 00 00 00 00  31 47 90 75 03 00 00 00  |........1G.u....|
00000030  08 00 00 00 00 00 00 00  82 70 6c 5d 03 00 00 00  |.........pl]....|
00000040  08 00 00 00 00 00 00 00  5a 01 bd 62 03 00 00 00  |........Z..b....|
00000050  08 00 00 00 00 00 00 00  38 77 97 4a 03 00 00 00  |........8w.J....|
00000060  08 00 00 00 00 00 00 00  c0 4e 41 5d 03 00 00 00  |.........NA]....|
00000070  08 00 00 00 00 00 00 00  4a 10 f2 44 03 00 00 00  |........J..D....|
00000080  08 00 00 00 00 00 00 00  39 28 cc 6e 03 00 00 00  |........9(.n....|
00000090  08 00 00 00 00 00 00 00  47 a5 bf 56 03 00 00 00  |........G..V....|
000000a0  08 00 00 00 00 00 00 00  50 d4 ac 75 03 00 00 00  |........P..u....|
000000b0  08 00 00 00 00 00 00 00  36 60 de 5d 03 00 00 00  |........6‘.]....|
000000c0  08 00 00 00 00 00 00 00  98 3c 95 74 03 00 00 00  |.........<.t....|
000000d0  08 00 00 00 00 00 00 00  bc 9c 96 5c 03 00 00 00  |...........\....|
000000e0  08 00 00 00 00 00 00 00  d3 bf c3 6b 03 00 00 00  |...........k....|
000000f0  08 00 00 00 00 00 00 00  3b fe 8d 53 03 00 00 00  |........;..S....|
```

add_device_randomness_time-usb_new_device

```
Time information
00000000  08 00 00 00 00 00 00 00  a8 0f c0 2f 03 00 00 00  |.........../....|
00000010  08 00 00 00 00 00 00 00  18 1e c0 2f 03 00 00 00  |.........../....|
00000020  08 00 00 00 00 00 00 00  48 68 c0 2f 03 00 00 00  |........Hh./....|
00000030  08 00 00 00 00 00 00 00  72 46 bb 2e 03 00 00 00  |........rF......|
00000040  08 00 00 00 00 00 00 00  63 54 bb 2e 03 00 00 00  |........cT......|
00000050  08 00 00 00 00 00 00 00  10 5c bb 2e 03 00 00 00  |.........\......|
00000060  08 00 00 00 00 00 00 00  bb e8 ed 2d 03 00 00 00  |...........-....|
00000070  08 00 00 00 00 00 00 00  4d f5 ed 2d 03 00 00 00  |........M..-....|
00000080  08 00 00 00 00 00 00 00  24 fd ed 2d 03 00 00 00  |........$..-....|
00000090  08 00 00 00 00 00 00 00  89 dc ca 2c 03 00 00 00  |...........,....|
000000a0  08 00 00 00 00 00 00 00  39 29 ca 2c 03 00 00 00  |........9).,....|
000000b0  08 00 00 00 00 00 00 00  a9 32 ca 2c 03 00 00 00  |.........2.,....|
000000c0  08 00 00 00 00 00 00 00  d8 6a 70 e2 04 00 00 00  |.........jp.....|
000000d0  08 00 00 00 00 00 00 00  28 76 70 e2 04 00 00 00  |........(vp.....|
000000e0  08 00 00 00 00 00 00 00  40 7e 70 e2 04 00 00 00  |........@~p.....|
000000f0  08 00 00 00 00 00 00 00  54 17 81 50 03 00 00 00  |........T..P....|
```

add_device_randomness_time-dmi_walk_early

Time information

```
00000000  08 00 00 00 00 00 00 00  af ba e4 90 03 00 00 00  |................|
00000010  08 00 00 00 00 00 00 00  3e d8 e4 90 03 00 00 00  |........>.......|
00000020  08 00 00 00 00 00 00 00  57 05 e4 90 03 00 00 00  |........W.......|
00000030  08 00 00 00 00 00 00 00  82 69 e3 af 03 00 00 00  |.........i......|
00000040  08 00 00 00 00 00 00 00  a3 87 e0 af 03 00 00 00  |................|
00000050  08 00 00 00 00 00 00 00  ad f3 e0 af 03 00 00 00  |................|
00000060  08 00 00 00 00 00 00 00  74 67 29 9d 03 00 00 00  |........tg).....|
00000070  08 00 00 00 00 00 00 00  2d 85 26 9d 03 00 00 00  |........-.&.....|
00000080  08 00 00 00 00 00 00 00  25 f1 26 9d 03 00 00 00  |........%.&.....|
00000090  08 00 00 00 00 00 00 00  53 eb 67 98 03 00 00 00  |........S.g.....|
000000a0  08 00 00 00 00 00 00 00  d2 07 67 98 03 00 00 00  |..........g.....|
000000b0  08 00 00 00 00 00 00 00  41 73 67 98 03 00 00 00  |........Asg.....|
000000c0  08 00 00 00 00 00 00 00  e9 67 2b a9 03 00 00 00  |.........g+.....|
000000d0  08 00 00 00 00 00 00 00  34 85 28 a9 03 00 00 00  |........4.(.....|
000000e0  08 00 00 00 00 00 00 00  6b f1 28 a9 03 00 00 00  |........k.(.....|
000000f0  08 00 00 00 00 00 00 00  66 9f 8d af 03 00 00 00  |........f.......|
```

add_device_randomness_time-posix_cpu_timers_exit

```
Time information
00000000  08 00 00 00 00 00 00 00  f5 cb 72 4b 03 00 00 00  |..........rK....|
00000010  08 00 00 00 00 00 00 00  2d a0 73 4b 03 00 00 00  |........-.sK....|
00000020  08 00 00 00 00 00 00 00  a5 c8 73 4b 03 00 00 00  |..........sK....|
00000030  08 00 00 00 00 00 00 00  bd 6a 73 4b 03 00 00 00  |.........jsK....|
00000040  08 00 00 00 00 00 00 00  51 96 70 4b 03 00 00 00  |........Q.pK....|
00000050  08 00 00 00 00 00 00 00  01 39 70 4b 03 00 00 00  |.........9pK....|
00000060  08 00 00 00 00 00 00 00  51 59 70 4b 03 00 00 00  |........QYpK....|
00000070  08 00 00 00 00 00 00 00  95 fb 71 4b 03 00 00 00  |..........qK....|
00000080  08 00 00 00 00 00 00 00  f9 1b 71 4b 03 00 00 00  |..........qK....|
00000090  08 00 00 00 00 00 00 00  81 86 6e 4b 03 00 00 00  |..........nK....|
000000a0  08 00 00 00 00 00 00 00  fd 2c 6e 4b 03 00 00 00  |.........,nK....|
000000b0  08 00 00 00 00 00 00 00  f9 56 6e 4b 03 00 00 00  |.........VnK....|
000000c0  08 00 00 00 00 00 00 00  19 fd 6f 4b 03 00 00 00  |..........oK....|
000000d0  08 00 00 00 00 00 00 00  b5 1d 6f 4b 03 00 00 00  |..........oK....|
000000e0  08 00 00 00 00 00 00 00  31 96 6c 4b 03 00 00 00  |........1.lK....|
000000f0  08 00 00 00 00 00 00 00  75 05 6c 4b 03 00 00 00  |........u.lK....|
```

Closer look

Statistics

add_device_randomness_time-__dev_open

- # of entries: 6136
- # of entry classes: 6136
- # of classes / # of entries ratio: 1.0
- avg # of 0x00 per entry: 3.0151
- lengths of entries: 8B

add_device_randomness_time-register_netdevice

- # of entries: 6136
- # of entry classes: 6136
- # of classes / # of entries ratio: 1.0
- avg # of 0x00 per entry: 3.0106
- lengths of entries: 8B

Closer look

Statistics

add_device_randomness_time-usb_new_device

- # of entries: 46020
- # of entry classes: 46018
- # of classes / # of entries ratio: 0.99996
- avg # of 0x00 per entry: 3.0279
- lengths of entries: 8B

add_device_randomness_time-posix_cpu_timers_exit

- # of entries: 932923
- # of entry classes: 932878
- # of classes / # of entries ratio: 0.99995
- avg # of 0x00 per entry: 3.0154
- lengths of entries: 8B

Graph

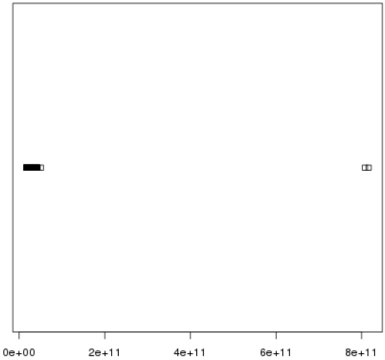


Figure: add_device_randomness_time-__dev_open

Graph

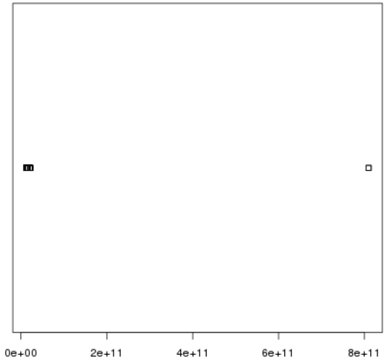


Figure: add_device_randomness_time-register_netdevice

Graph

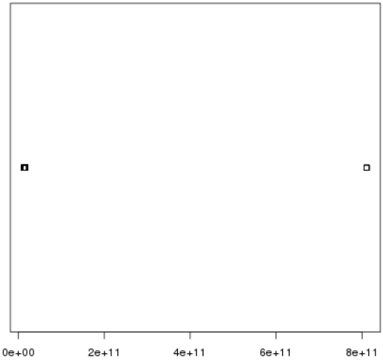


Figure: add_device_randomness-dmi_walk_early

Graph

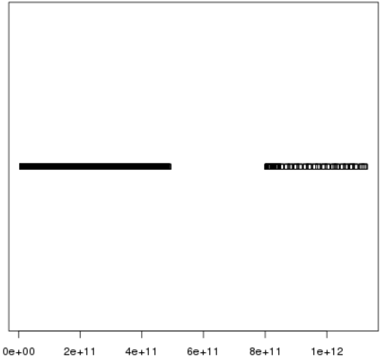


Figure: add_device_randomness_time-posix_cpu_timers_exit

Graph

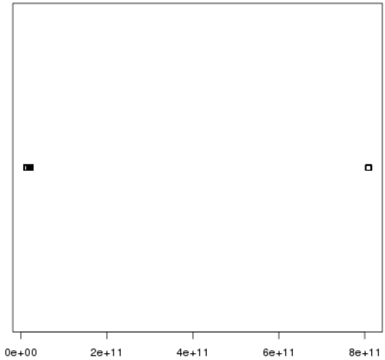


Figure: add_device_randomness_time-usb_new_device

Graph

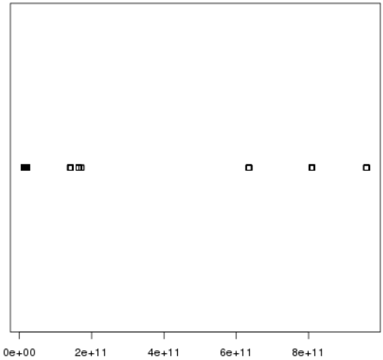


Figure: add_device_randomness_time-usb_new_device

Future Plans

- Explore differences between different virtual machine hosts

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance
- Use openstack API to automate data collection

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance
- Use openstack API to automate data collection
- Further analysis of data

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance
- Use openstack API to automate data collection
- Further analysis of data
- Compute entropy of larger data sets

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance
- Use openstack API to automate data collection
- Further analysis of data
- Compute entropy of larger data sets
- haveged - A simple entropy daemon

Future Plans

- Explore differences between different virtual machine hosts
- Create openstack image
  based on current kernel, probably fedora 21
- Execute data collection in openstack instance
- Use openstack API to automate data collection
- Further analysis of data
- Compute entropy of larger data sets
- haveged - A simple entropy daemon
- GNU rng-tools

Other Works

- Filip Škola - Bachelor thesis
- Ondřej Mokoš - Master thesis

Thanks

Thank you for your attention.

Bibliography I

- Patrick Lacharme et al. *The Linux Pseudorandom Number Generator Revisited*. Cryptology ePrint Archive, Report 2012/251. http://eprint.iacr.org/. 2012.
- Filip Škola. *Semínko generátoru náhodných čísel OS Linux při bootu*. 2012. URL: https://is.muni.cz/th/325197/fi_b.
- Ondřej Mokoš. *Analýza entropie dat sloužících jako semínko generátoru náhodných čísel OS Linux při bootu*. 2013. URL: https://is.muni.cz/th/208173/fi_m/.