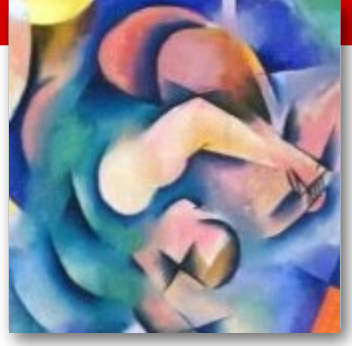
/dev/random and SP800-90B

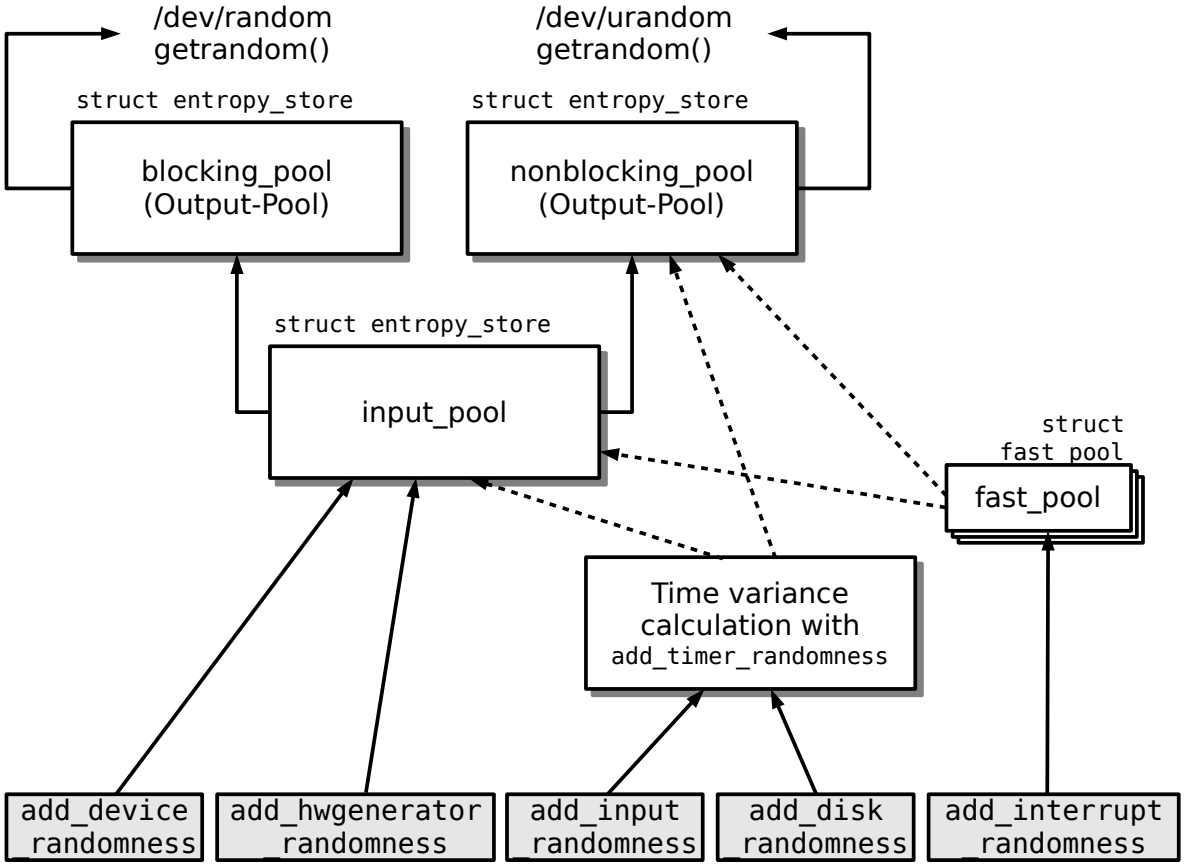
Stephan Müller <stephan.mueller@atsec.com>

Agenda

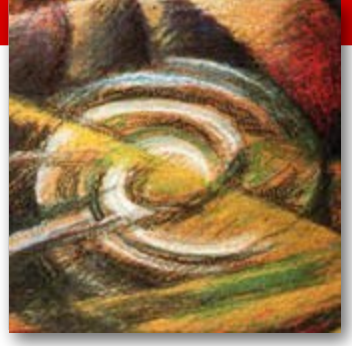


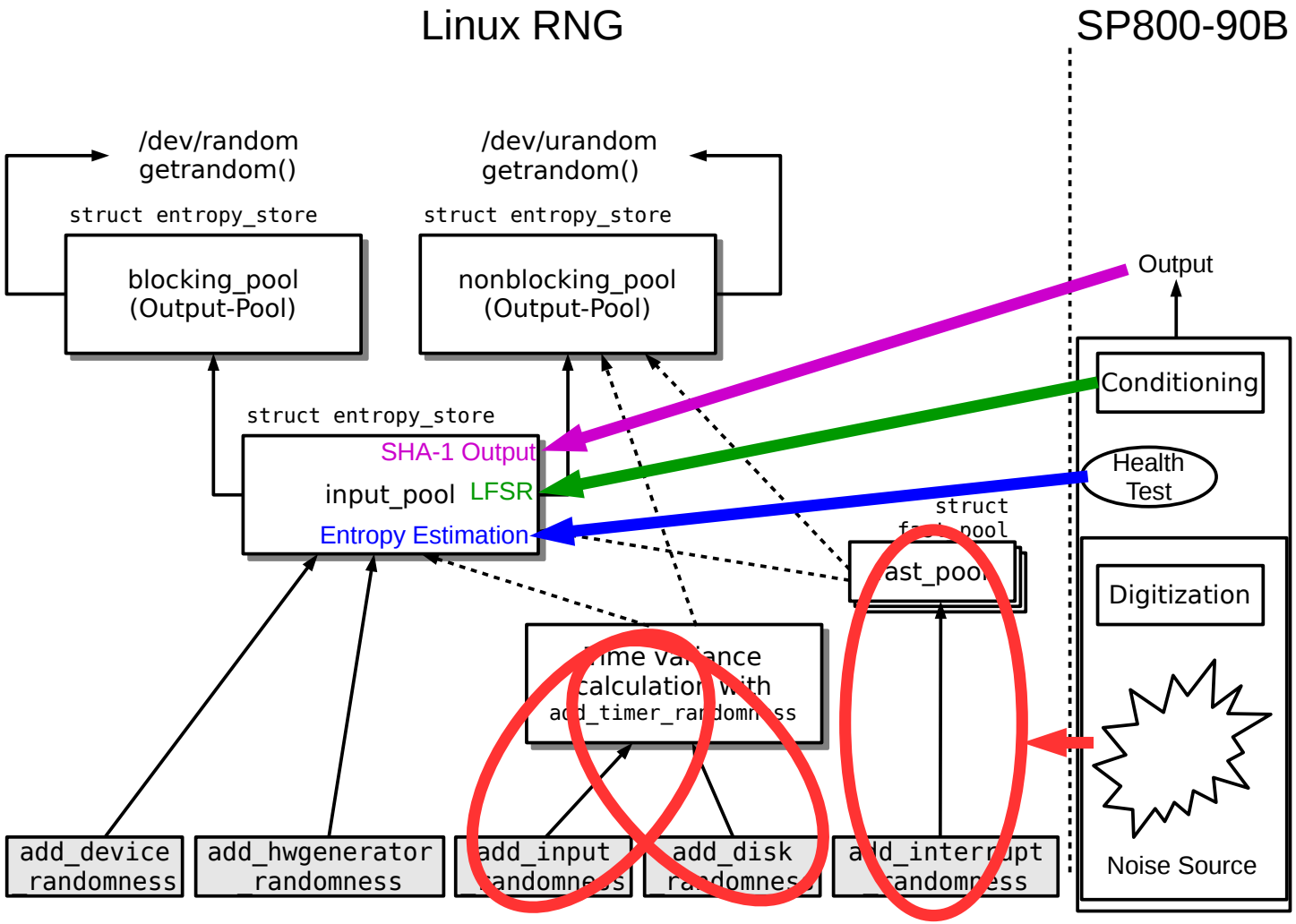
- Linux RNG applied to concepts of SP800-90B chapter 4
- Noise source assessment based on SP800-90B section 6.3
- Conditioner assessment based on SP800-90B section 6.4
- Health test assessment based on SP800-90B section 6.5
- Test approach discussion
- Test for IID based on SP800-90B section 9.1
- Entropy estimation based on SP800-90B section 9.3
- Concluding remarks on SP800-90B

Recap: /dev/random Architecture



Mapping of Linux RNG and SP800-90B





Linux RNG Noise Sources

- Disk I/O
  - Block Device Number + 0x100 || Jiffies || High-Resolution Timer
  - Noise derived from access times to spinning platters
- Human Interface Devices (HID)
  - Event Number || Jiffies || High-Resolution Timer
  - Noise derived from human interaction
- Interrupts
  - fast_pool: 4 32-bit words filled with
    - Jiffies
    - High-Resolution Timer
    - IRQ Number
    - 64 bit Instruction Pointer of the CPU
  - fast_pool mixed into input_pool once per second or after 64 received interrupts – whatever comes later
    - Goal: Break correlation with disk / HID events

Linux RNG Conditioner

- Conditioner mixes data into input_pool
- Non-approved mechanism according to SP800-90B
- LFSR for 128 * 32-bit pool with full rank polynomial
  - $x^{128} + x^{104} + x^{76} + x^{51} + x^{25} + x + 1$
- Goal: Bias reduction
- Disk / HID: Bias added due to structure of data to be mixed into input_pool with:
  - MSB with rather static data (event numbers)
  - Middle bits with low entropy data (Jiffies)
  - LSB with high-entropy data (high-resolution timer)

Linux RNG Health Test

- Disk, HID: 1st, 2nd, 3rd derivation of event time in Jiffies
  - Minimum of all derivation is estimated entropy of event
  - Limitation to 11 bits maximum per event
    - → Claim: one bit of input data has less than one bit of entropy
    - → Covers continuous health test requirement
    - → Covers repetition count requirement
  - Derivation is applied to all events → covers start-up health test requirement
- Interrupts: Implicit—without interrupt handling there is no live Linux kernel
  - Exactly one bit of entropy estimated per injection into input_pool
    - → Claim: one bit of input data has less than one bit of entropy
    - → Covers continuous health test requirement
    - → Covers start-up health test requirement
    - → No repetition count check
- No Adaptive Proportion Test—entropy measurement considered equivalent
- Goal of identifying failures is met

Obtaining Raw Data

- How to observe noise sources and LFSR / input_pool?
  - In a live Linux kernel
  - Unchanged Linux kernel
  - Measurement shall not impact entropy calculation
- Answer: SystemTap
- Heisenberg's uncertainty still applies
  - SystemTap changes timing by adding additional code paths

    → Akin to executing Linux on a slower system

    → No impact on entropy calculation

Quantitative Test

- SystemTap scripts
  - Recording noise sources with
    - Disk / HID: event number, Jiffies, high-res timer

      8388864 4463110016 1925778664
      8388864 4463110031 1968130017
      8388864 4463110031 1968494953
    - Interrupts: 4 32-bit values at mix-in time into input_pool

      437329669 643088605 2692866823 866121204
      1344373354 878662894 1014397613 3814229428
      1586927008 1317385070 1476249883 3526254608
  - Recording of input_pool snapshots after 128 bytes of input data

    1678657432 743891205 2464344685 329492648 1033032366 3229210488 305531768 569196974 3652500464 3634893
    1146826902 2400579469 49319170 4034419946 2180769455 279336902 2880243547 934715568 4273575111 1752953336
    2298729067 2917205949 102492675 2404838404 2353180084 2969558238 641044075 1232241451 1006621227
    1991954106 3617754453 41628629 1866532308 1076027776 769853502 4084160734 2821261083 397415737 2583539674
    3061094309 2475036122 2248823388 6981325 2486620015 915556753 3542571149 3911010330 2330971665 2527449554
    1721046704 3644547758 1289293266 3263421274 2329535655 2977626513 503131610 2184559219 2681631171 18858674
    2147950528 2354863804 3552431347 2361759624 1718845983 2874468454 1414016530 2147555820 1959716200
    276062261 2542827259 2156853529 3952119267 3235420817 1306250092 2117738582 1522266350 1173864654
    4198594590 3265047086 491683108 3896066180 2189371639 90794119 3716741233 872257793 3981505182 4019402506
    453076263 1279402849 2550514005 3576952212 309224290 4108881444 2010691797 956332919 1148238251 1272549368
    1105383894 240296969 206403260 3831557685 3277834103 2666820462 2343544165 2615020452 3739270272
    3194697506 362529807 3083490420 6938878 3656915489 189919126 3612917688 3761622739 2223431215 3483126322
    368477673 203121163 3393308254 3502245948 1414163483 3653111022 1552685444 70033309 2242958265 1669436413
    2184958501 235125957

Test Results Noise Sources IID

- General: Chi-Square for IID cannot be calculated
- General: Chi-Square Goodness Fit cannot be calculated
- Disk / HID
  - Only high-resolution timer tested due to main entropy source
  - Non-IID based on SP800-90B tests section 9.1
  - Using low 11 bits of timer → data is almost IID
- Interrupts
  - Each 32-bit word is tested individually
  - About half of IID tests fail → non-IID

Test Results Noise Sources Entropy

- General: collision tests N/A due to no collisions
- General: All sanity checks always pass
- Disk
  - Compression test: Mean: 15.2, Sigma 1.3, Min Entropy: 16.6
  - Frequency test: Mean: 30.5, Sigma 1.5, Min Entropy: 8
- HID
  - Compression test: Mean: 15.2, Sigma 1.3, Min Entropy: 16.6
  - Frequency test: Mean: 30.5, Sigma 1.5, Min Entropy: 8
- Interrupt
  - Compression test: Mean: 15.1 – 15.2, Sigma 1.2 – 1.6, Min Entropy: 12.6 – 16.6
  - Frequency test: Mean: 30.5, Sigma 1.5 – 1.6, Min Entropy: 7.1 – 8.4

Test Results Conditioner IID

- General: Chi-Square for IID cannot be calculated
- General: Chi-Square Goodness Fit cannot be calculated
- Calculation performed for one word
- About half of IID tests fail → non-IID

Test Results Conditioner Entropy

- General: collision tests N/A due to no collisions
- General: All sanity checks always pass
- Compression test: Mean: 15.2, Sigma 1.3, Min Entropy: 16.6
- Frequency test: Mean: 30.5, Sigma 1.5, Min Entropy: 8
- Other entropy tests cannot be calculated

RNG good enough?

- Noise sources: Using the min entropy values for events and considering the maximum of 11 bits of entropy estimated per event, we **pass** SP800-90B.
  - Additional testing beyond SP800-90B shows:
    - More than 60% of events are estimated to have 0 bits of entropy
    - About 20% of events are estimated to have 1 bit of entropy

      → massive underestimation of entropy in noise sources
- Conditioner: No change from noise sources

  → With entropy estimator enforced when obtaining random values—preventing of random number output when too little noise is present—the passing of the noise source implies passing of the entire random number generator.

  → Statement applies to input_pool!

  → Other pools feeding /dev/random and /dev/urandom are DRNGs!

Comments on SP800-90B

- Assumption of a certain structure of an entropy source
  - Straight data path from noise source to output
  - Difficult to apply to noise sources maintaining an entropy pool
- Conditioner is assumed that it generates data and outputs it
  - When using entropy pool, there are distinctions between
    - State transition function (conditioner operation)
    - Output function
- Health test assumes that a binary decision is made on noise source
  - /dev/random does not use binary decision
- Mathematical description of calculating entropy in 9.3 is not clear
- Chi-Square test definition is insufficient
  - Applying a different method with 4 bit nibbles per measurement, Chi-Square can be calculated (e.g. for input_pool p is between 15% and 88%)

Uncovered

- /dev/urandom
- Non-x86 systems
- Virtual environments
- Jitter RNG