Pseudorandom Number Generation in Linux

Zane Goldhahn (p72n371)
Garrett Perkins (m95m353)
Ethan Fison (t85j427)
John Dolph (r87f693)

11/15/2020

Outline

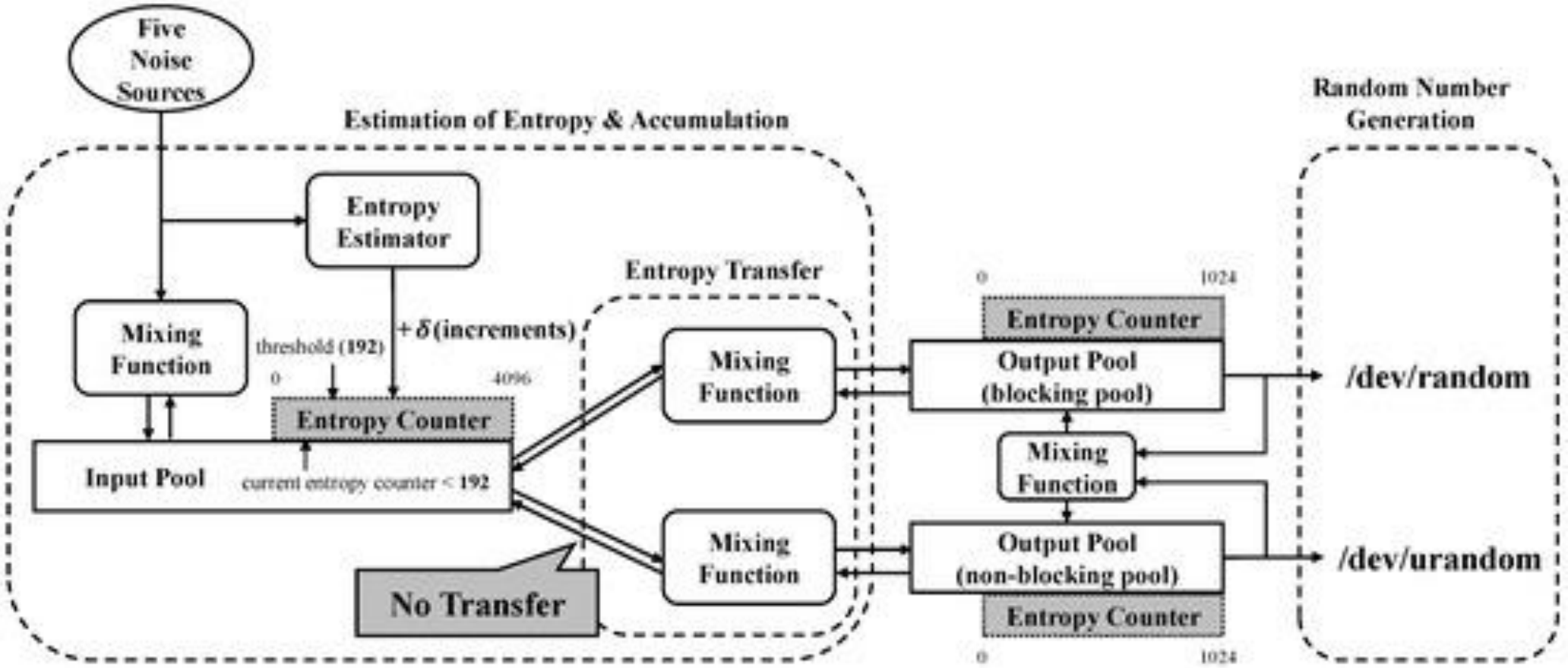
- Motivation
- Overview of Linux PRNG
- Entropy Collection
- Cryptographic Algorithms
- Hardware Random Number generation
- Random Number Extraction Demo

Why do we care?

Applications of Random Numbers:

- Monte Carlo Simulations
  - Often used in finance, e.g. options pricing [3]
- Cryptography
  - e.g. RSA keys [2]

Linux PRNG Overview



Source [1]

Entropy Collection

Source [5]

- Entropy is collected from indeterministic sources
- Entropy is mixed into the input pool
- Number of bits of entropy provided by event is estimated

SHA-1 Hash Algorithm

- Produces a fixed-size, irreversible output value based on a variable-size input.

- Introduces a characteristic of randomness: the output may not be traced back to an initial state.

Entropy Mixing Algorithm

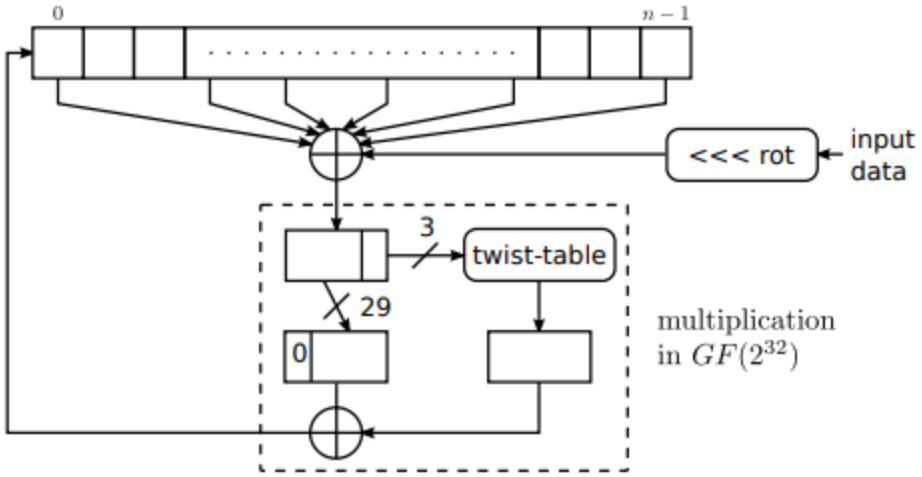


Figure 3: The mixing function.

- Provides a method of ensuring the entropy pool has a high amount of entropy.
- An attacker may possess some insights related to the data processed with low entropy. There should be no predictability associated with the internal system state.

Diagram Source: See [4]

Entropy Extraction Algorithm

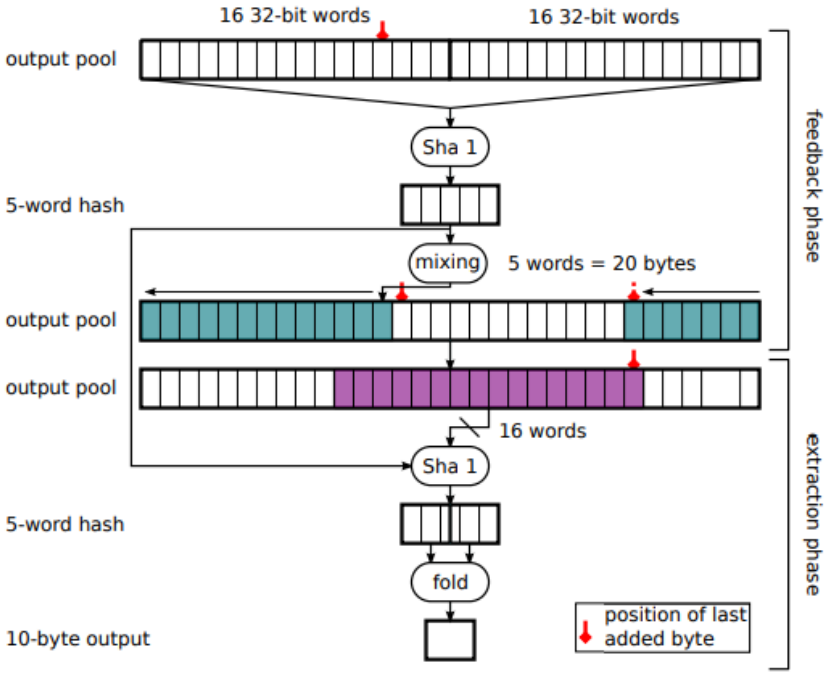


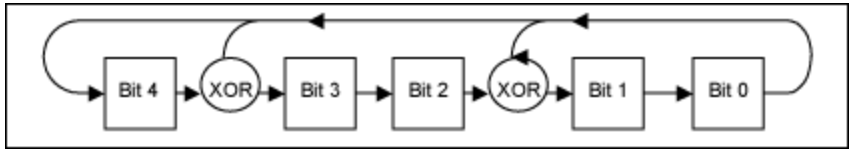
Figure 5: The output function of the Linux PRNG.

- Facilitates the transfer of entropy between functions and entropy pools.
- Delivers random data for use by applications.
- The final outputs are delivered to /dev/random or /dev/urandom.

Diagram Source: See [4]

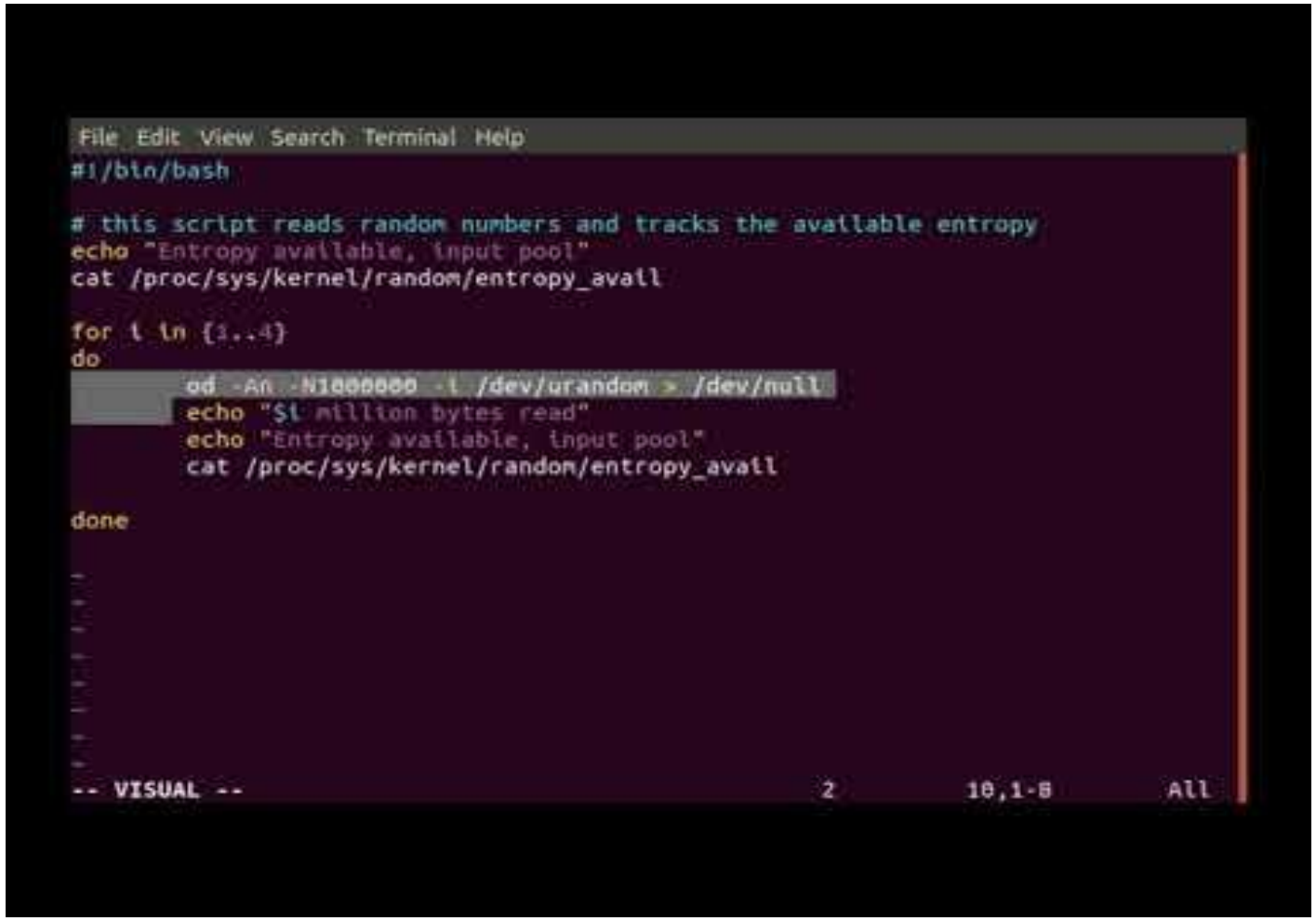
Hardware-level RNG

- No HRNGs for Linux
  - There is support
- Linear Feedback Shift Registers (LFSRs)



- RNG on CPUs and other chips
- FPGA RNGs

Demo


File Edit View Search Terminal Help
#!/bin/bash
this script reads random numbers and tracks the available entropy
echo "Entropy available, input pool"
cat /proc/sys/kernel/random/entropy_avail
for i in {1..4}
do
od -An -N1000000 -i /dev/urandom > /dev/null
echo "$i million bytes read"
echo "Entropy available, input pool"
cat /proc/sys/kernel/random/entropy_avail
done
-- VISUAL --
2
10,1-8
All

Conclusion

- What we've covered
- Where to find more information

References

[1] *"Recoverable Random Numbers in an Internet of Things Operating System,"* Accessed on: Nov. 13, 2020. [Online]. Available: https://www.mdpi.com/1099-4300/19/3/113/htm

[2] *"Ron was wrong, Whit is right,"* Accessed on: Nov. 14, 2020 [Online]. Available: https://eprint.iacr.org/2012/064.pdf

[3] *"Option Pricing - Monte-Carlo Methods,"* Accessed on: Nov. 14, 2020 [Online]. Available: https://www.goddardconsulting.ca/option-pricing-monte-carlo-index.html

[4] *"Entropy Management Diagrams,"* Accessed on: Nov. 10, 2020. [Online]. Available: https://eprint.iacr.org/2012/251.pdf

[5] *"Ensuring Randomness with Linux's Random Number Generator,"* Accessed on: Nov. 14, 2020 [Online]. Available: https://blog.cloudflare.com/ensuring-randomness-with-linuxs-random-number-generator/